Software Engineering Institute

Job Analysis Results for Malicious-Code Reverse Engineers: A Case Study

Jennifer Cowley

May 2014

TECHNICAL REPORT
CMU/SEI-2014-TR-002

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon University

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0001119

Table of Contents

List of Figures

List of Tables

Abstract

Recently, government and news media publications have noted that a large-scale military cyberattack against the United States will be crippling primarily because of the existing personnel shortages and expertise gaps in the cybersecurity workforce. One critical job role within cyber defense teams is the malicious-code reverse engineer who deconstructs malicious code to understand, at the binary level, how the malware behaves on a network. Given the severe staffing shortages of these engineers, efforts to identify individual traits and characteristics that predict the development of expertise is important. Currently, job analysis research on teams of malicious-code reverse engineers is lacking. Therefore, a job analysis was conducted to identify individual factors (e.g., cognitive abilities, knowledge, and skills) and team factors (e.g., team leadership, decision making) that enable, encumber, or halt the development of malicious-code reverse engineering expertise. A 10-member malicious-code reverse engineering team was interviewed using a contextual inquiry/semi-structured interview hybrid technique to collect job analysis information. Performance factors were inferred based on the raw interview data.

The results indicate that expert performance requires other non-domain-specific knowledge and skills (e.g., performance monitoring, oral and written communication skills, teamwork skills) that enable successful performance. Expert performance may be enabled by personality factors (i.e., conscientiousness) and cognitive abilities (i.e., working memory capacity). Attributes of successful novices were also collected. Subsequent research will empirically validate that these factors predict the development of expertise. Training and operations implications for this research are also detailed.

1 Introduction

Recently, government and news media publications[1] have noted that a large-scale military cyberattack against the United States will be crippling primarily because of the existing personnel shortages and expertise gaps in the cybersecurity workforce [Evans 2010]. Consequently, the mission of the U.S. Department of Defense's (DoD's) Science and Technology Enterprise [DoD 2011] includes the acceleration of trained, future, workforce personnel [DoD 2010]; however, training the masses is resource intensive (e.g., time, money, manpower). A more advantageous approach is to train personnel with the greatest potential to rapidly excel in training paradigms that mimic real-world job tasking rather than train the masses. One way to identify potential candidates is using an operator selection program (OSP)—a method of selecting individuals into training programs based on a matched profile between the individual's capabilities and previously validated, predictive performance capabilities. The research methodology used to establish an OSP has been extensively used and validated in other domains such as aviation [Nickels 1995, Nyfield 1983], rail transportation [Shapiro 2013], human resources [Hausdorf 2010, Kuncel 2010], and military personnel selection [Halstead 2008, White 2005]. OSPs are typically established to select candidates with the greatest potential of becoming experts[2] in mission-critical jobs with severe staffing shortages. One such job role that is the lynchpin of cyber defense teams [DoD 2010, slide 14] is the malicious-code reverse engineer (also called a malicious-code analyst or malware analyst) who deconstructs malicious code to understand, at the binary level, how the malware behaves on a network. Given the severe shortages of people in this important job role [Sikorski 2012, p. XXViii], we aim to establish an OSP to identify a profile of individual traits and characteristics that can predict expert on-the- job performance.

Historically, OSP research has exclusively studied cognitive abilities as performance predictors [Thomas 2006]. However, recent critiques on the low validity of these cognitive ability performance predictors in OSPs have pushed the research community to include measures of non-cognitive psychological factors (e.g., emotional intelligence, personality, integrity, social desirability) in an attempt to improve predictive validity [Lievens 2011, Stabile 2002, Thomas 2006]. One non-cognitive psychological factor receiving little attention in OSP research is teamwork skills, which we loosely define here as human skills or attributes that facilitate effective team member interactions to accomplish a team mission or goal. A large corpus of teamwork research external to OSP research indicates that teamwork skills are important to job performance in many present-day organizations [Cohen 1997, Lee 2013, McKendrick 2013, Yilmaz, 2013]. In addition, teamwork skills are listed in the task work outlined in various cybersecurity job analysis findings in the development of a DoD Cyber Workforce Framework created by the National Initiative for Cybersecurity Education [DHS 2012]. While this prior job analysis research lacked information on the job role of malicious-code reverse engineer, the relationship this job role has with forensics and incident handling implies some level of teamwork. Therefore, what is missing in OSP re-

[1] "Less than ten percent of the estimated necessary 30,000 skilled security professionals are in the workplace – it is clear that addressing the gap has never been greater," according to SANS NewsBites Volume 14, Number 54, dated 7/10/12.

[2] The term *expert* is loosely defined as a person possessing a comprehensive and authoritative knowledge of or skill in a particular area. We will expand this definition later in this technical report.

search is not only job analysis research on malicious-code reverse engineering but also the study of teamwork skills as potential predictors of reverse engineer job performance.

If the overall purpose of this work is to find job candidates who possess the greatest potential of developing expertise rapidly, an exclusive focus on individual selection criteria may encumber the overall objective of OSPs. Hence, a holistic evaluation is warranted of other organizational and team factors that can adversely impact training and on-the-job performance [Arvey 1998, Guzzo 1996]. In other words, the selection of qualified individuals based on individual traits and characteristics is moot if the organizational and team contexts do not support the development of their expertise.[3] Prior teamwork research has indicated that organizational contexts are one of the primary inhibitions to the development of individual and team expertise [Drouin 2013, Tannenbaum 2012, Voss 1995]. Organizational cultures, philosophies, and policies can encumber team skill acquisition and team performance [Seamster 2001, Tannenbaum 2012]. In addition, team performance can be adversely impacted by teamwork factors such as a lack of team trust [Lee 2013], lack of team mental models [Edwards 2006, Lim 2006, Marks 2000, Mathieu 2000], lack of team transactive memory[4] [Akgün 2005, Austin 2003, Gino 2010, Zhang 2007], poor communication [Jentsch 2001, McIntyre 1995], and lack of effective team leadership [Bass 1985, Ginnett 1987]. In addition, theories outlining components of effective teamwork [Dickinson 1997], as well as teamwork competencies [Cannon-Bowers 1995], have been generated. Therefore, the OSP research effort reported here seeks to identify organizational contexts and team factors that enable, encumber, or halt the development of an individual's expertise.

The first step in establishing an OSP is to conduct an extensive job analysis of a team of malicious-code reverse engineers. Job analysis results will be used to generate possible performance predictors that we call *potential requirements (PR)*. These PRs formulate the profile of organizational, team, and individual factors (e.g., characteristics, traits, qualities, capabilities) that may impact personnel selection and rapid development of expertise. The term *PRs* was intentionally chosen for several reasons. First, we are evaluating a system of expertise development that includes humans, technology, and organizational contexts. The term *requirements* has traditionally been reserved for non-human system components; we are expanding the use of this term to include socio-technical system components (e.g., humans, computers, and organizations). In addition, this study is not generating competencies[5] because they focus exclusively on the individual and are not defined in terms of the team or organizational impacts. Finally, requirements are labeled *potential* because they are not validated on a broader sample of malicious-code reverse engineers. Validation research will be done in follow-on research.

To summarize, we aim to identify potential requirements of the job role of malicious-code reverse engineer and respective organizational and team contexts that impact and potentially predict the

[3] Five levels of expertise exist on a continuum from novice, apprentice, journeyman, expert, and finally to master. The development of expertise is the individual improvement from lower levels of expertise towards higher levels of expertise (expert and master). Clark defines an *expert* as a person whose judgments are uncommonly accurate and reliable, whose performance shows both skill and economy of effort, and who deals with tough and unusual cases. A master teaches others whose judgments set regulations, standards, or ideas [Clark 2008, p. 8]. In this technical report, we use the term *expert* for both the expert and master levels of expertise.

[4] *Transactive memory* is the practice of dividing up the total human memory information load such that each team member holds in his or her memory a subset of information required for team performance.

[5] *Competencies* are underlying characteristics of a person that result in effective and/or superior performance in a job [Boyatzis 1982].

rapid development of incumbent expertise. This initial research will be the foundation of an OSP for malicious-code reverse engineers.

This report is structured as follows:

- Section 2 details the study methodology used as well as participant sampling.
- Section 3 provides an overview of the analyses used and the results.
- Section 4 summarizes the results, implications, and limitations of the research.
- Section 5 details unexpected research challenges that have implications for academic researchers and operations.

2 Method

Several step-by-step job analysis protocols exist in OSP research paradigms; however, we chose an adapted version from the U.S. Federal Aviation Administration's (FAA's) job analysis protocols documented by Doverspike and Arthur [Doverspike 2012] and Nickels and colleagues [Nickels 1995]. Our adapted protocol includes the following steps:

1. Review existing literature (e.g., peer-review publications on job analysis within cybersecurity, job descriptions, source materials, other published job analysis literature on cybersecurity jobs) and assemble a list of job tasks or other relevant job analysis information.
2. Conduct job analysis interviews and analyze the results.
3. Validate the list of job tasks with a focus group on subject matter experts.
4. Create and launch a survey of incumbents to rate the importance and frequency of each job task and requirement.
5. Analyze the results using descriptive models and a linkage diagram.
6. Cull the results to obtain a parsimonious task list and set of job requirements based on Steps 4 and 5.

This document reports on Steps 1 and 2 and details them below; future research will report on Steps 3-6.

2.1 Step 1. Review existing literature.

2.1.1 Purpose and Overall Description

The purpose of this step is to collect published job analysis information (e.g., task lists, job requirements) on malicious-code reverse engineer roles to build a foundation list of task work and potential predictors.

2.1.2 Method

We conducted a modified systematic literature review [Kitchenham 2009] to identify all the research papers analyzing the job of malicious-code reverse engineer. We searched the peer-reviewed literature in Google Scholar using all two-way permutations following two groups of key word terms: (1) job analysis, work analysis, job task analysis, and cognitive task analysis and (2) reverse engineering, malicious-code reverse engineering, and malware analyst. When no results were produced, we broadened the search to include any publications on cybersecurity job analysis in the public domain. We subsequently searched Defense Technical Information Center (DTIC) for public research papers on malicious-code reverse engineers, and, when that produced no results, we broadened the search again to include publications on cybersecurity job analysis. We found these six non-peer-reviewed publications of job analyses on cybersecurity job roles, but none included the malicious-code reverse engineer job role:

- *O*Net™*
- *Bureau of Labor Statistics Occupational Outlook Handbook*
- *Development of a DoD Cyber Workforce Framework*
- *OPM Job Family Standards in the Information Technology Group*

- *National Initiative for Cybersecurity Education (NICE)*
- *DoD 8570 Information Assurance Workforce Improvement Program*

All cybersecurity job roles and respective tasks listed in the above documents were aggregated into a single list of 969 total tasks; redundancies were included in this total count. None of the above publications included the malicious-code reverse engineer job role, yet two job roles (computer network defense [CND] incident responder and CND forensics analyst) from two different sources listed task duties involving malware (see Table 1). Given that these results were not useful for providing an understanding of the task work of malicious-code reverse engineers, we proceeded to the next step of our protocol listed in the method section.

Table 1: Tasks Involving Malicious-Code Reverse Engineering or Malware Analysis from Resultant Systematic Literature Review

Task	Source	Job Role
Perform tier 1, 2, and 3 malware analysis.	*Development of a DoD Cyber Workforce Framework* (U.S. National Security Administration [NSA])	CND forensic analyst
Collect and analyze intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential CND incidents within the enclave.	*Development of a DoD Cyber Workforce Framework* (NSA)	CND forensic analyst
Collect and analyze intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential CND incidents within the enclave.	*Development of a DoD Cyber Workforce Framework* (NSA)	CND incident responder
Collect and analyze intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential CND incidents within the enterprise.	*NICE* document (functional roles)	CND incident responder

2.2 Step 2. Conduct job analysis interviews and analyze results.

2.2.1 Purpose and Overall Description

The purpose of this step is to generate individual, team, and organizational PRs based on the job analysis results that facilitate the rapid development of expert malicious-code reverse engineers. Since limited training exists for these reverse engineers, the development and measurement of expertise is assumed to exclusively occur on the job rather than in training facilities. We interviewed a team of malicious-code reverse engineers individually to collect job task work, knowledge/skill requirements, and work flow information. Then, we abstracted PRs from our analysis of the interview data.

2.2.2 Method

2.2.2.1 Participants

A 10-member team of self-identified reverse engineers and supporting staff[6] were interviewed: 4 junior malicious-code reverse engineers, 4 senior malicious-code reverse engineers, 1 trends ana-

[6] Supporting staff includes other professionals working intimately with malicious-code reverse engineers (i.e., researchers, trend analysts, and team leads) but does not include administrative assistants.

lyst, and 1 team manager. Not all members of the team self-identified as being full-time reverse engineers; however all knew how to reverse-engineer malicious code on some level and worked intimately with malicious-code reverse engineers. Table 2 depicts the type of work (i.e., trend analysis, longitudinal analysis, reverse engineering, and management) each team member is responsible for and the relative time commitment to each work type. Each row represents a single team member, whose identity has been anonymized to protect participant privacy.

Table 2: Type of Work and Respective Time Commitment of Each Team Member

Trends	Longitudinal	Reverse Engineering	Management
		x	xxx
xxx			
		x	
	xxx	xx	
xxx		x	
xx	xxx	xx	
	xx	xxx	x
xx		x	
		x	
x		xxx	
		xxx	
	xx	xxx	
KEY: x = some xx = much xxx = most			

2.2.2.2 Interview Materials

The interview strategy is an amalgamation of a semi-structured interview[7] and a contextual inquiry interview.[8] All interview materials provided in Appendix C were administered orally. Given the exploratory nature of this interview, each interview question was intended to inspire further discussion on the topic(s) the question presented.

The semi-structured interview materials are an agglomeration of content on the following topics:

1. participant's background
2. skills/knowledge requirements for novices and experts
3. critical incidents
4. teamwork
5. personality
6. organizational attributes

---

[7] A *semi-structured interview* is a "question/answer" interview strategy that allows for discussions of responses and mild deviations off-topic to important information.

[8] A *contextual interview* involves a researcher shadowing the participant doing work in the native work environment. Some questions can be asked of the participant to clarify the work being executed, but this interview technique does not include a predefined question set.

The participant's background content included questions to uncover historical individual attributes (e.g., work history, educational history, work experiences) important to developing expertise in entry-level reverse engineers. This information led to a discussion about what participants believed were the observable distinctions between expert and novice malicious-code reverse engineers, as well as the knowledge and skill requirements necessary for both types. Experts were defined as individuals who were superior to most senior reverse engineers, and novices were defined as entry-level new hires with little or no prior reverse engineering experience.

Since formal discussions with study participants did not produce distinctions between different cognitive abilities, the research team inferred cognitive ability requirements from the critical incidents provided. *Critical incidents* are accounts of experiences where unsafe acts or near-miss accidents occurred [Sanders 1987]. However, we adapted the critical incident technique to include examples of both poor and excellent reverse engineering job performance. To identify cognitive ability requirements, we discussed the natural abilities and talents of individuals involved in the examples of excellent reverse engineering performance.

The questions about teamwork and personality that we included (also provided in Appendix C) explored potential impactful factors to reverse engineer job performance that were identified in prior research. Teamwork question content included items about leadership styles [Bass 1997] and teamwork components [Dickinson 1997]. We verbally defined each leadership style investigated (i.e., laissez-faire, participative, consultative, democratic, and autocratic) and then asked participants to identify the most frequent leadership style(s) used within the team. Discussions about these styles followed. Next, we verbally defined teamwork components (i.e., team orientation, leadership, communication, monitoring, feedback, backup behavior, and coordination [Dickinson 1997]) and collected ratings of importance and frequency on questions representing each of them. Personality questions were generated based on the dimensions of the "Big Five" personality factors [Costa 1992] as well as other related information identified in the interview pilot testing. After verbally defining each of the five factors (i.e., openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism), we collected ratings of importance and frequency. More important than ratings, these five factors also served as discussion points to explore how personality may impact expertise development and what personality attributes seemed to be common among experts; thus, a more rigorous investigation into personality subscales was not explored.

A portion of the semi-structured interview questions was adapted from five out of the six dimensional question sets listed in the O*Net™ content model (http://www.onetcenter.org/content.html). These five dimensions include worker requirements, worker characteristics, experience requirements, occupational requirements, and occupation-specific information. We selected questions pertaining to organizational factors of white-collar jobs and used them to generate discussion in the organizational factors portion of the semi-structured interview.

We also conducted a contextual inquiry to assess task work, work flow, and communication patterns among team members. *Contextual inquiry* is a type of participant-shadowing technique to observe daily task work performed by the participant. Given the sensitive nature of reverse engineering work, a mock work environment was erected. That environment included a large monitor, a keyboard, a mouse, and office furniture typically found in participants' work environment; all

environmental artifacts served to cue memories of daily task work. Since contextual inquiries are unscripted, there are no associated interview materials in Appendix C.

2.2.2.3 Procedure

Prior to each two-hour interview, all participants were instructed to review the consent form and bring laptop computers to the mock work environment. After obtaining each participant's informed consent, we audio recorded each session for transcription and data-analysis purposes. At the beginning of each session, we reviewed the study's purpose and the interview agenda (i.e., Structured Interview Topics listed in Appendix C). During the final five minutes of each interview, we summarized the session's results and asked participants to critique the summary for accuracy. Then, we debriefed participants on the study objectives and compensated them for their time before releasing them.

Because of the large amount of content to cover in a single session, we were typically able to cover only about three-fourths of the content during each two-hour interview. All participants were asked questions on core topics (background information, knowledge requirements, and critical incidents), but coverage of other content areas was opportunistic such that we ensured at least two participants responded to each of those non-core content areas. The interview question order was largely participant-driven; for example, if a participant discussed teamwork concerns during the contextual interview, we followed up with teamwork questions.

3 Analysis Method and Results

In this section, we briefly describe our analysis method and then review the results of our analysis.

3.1 Analysis Method

The raw data collected in these interviews will help us generate PRs on the individual, team, and organizational strata for developing expertise in malicious-code reverse engineering. Raw data consists of statements made by a single interviewee about a particular concept or idea; we collated statements from multiple participants on each concept into a *raw data point*. Then, we annotated each point with the following example notation: P1-14, where *P1* identifies the individual and *14* is the comment number in the transcript attributed to that participant. We cite the raw data using this notation in the "Analysis Results" section below.

We used those data points to generate three descriptive models: (1) an affinity model [Kawakita 1975] that organizes the raw data into a taxonomic structure, (2) a communication flow model [Beyer 1998] that depicts the flow of information across all members of the malicious code team, and (3) the culture model [Beyer 1998] that documents the within-organization influences on the malicious code team. Because the information contained in these descriptive models was proprietary, we could not publish the models.

Each insight[9] gleaned from review of the raw data and models was translated into one or more PRs. A single PR can address the raw data points made by one or more interview participants. We wrote most of the PRs as statements that follow the grammatical structure below. However, the level of granularity of all PRs was not consistent because raw data represent different levels of granularity:

- **summarizing category:** an overall requirement descriptor
  for example, *Minimal distractions from task engagement*
- **objective:** the goal or purpose behind the actions
  for example, *To foster the development of expertise*
- **actions:** processes, procedures, and so forth articulated to achieve said objective
  for example, *Minimal distraction from deep engagement with the work and problem space is important.*
- **intent:** the underlying reasoning or rationale for why the actions are needed to achieve the objective or why this potential requirement is important
  for example, *Distractions reduce the time available to work on problems*

[9] An *insight* is an understanding of relationships between raw data that may further clarify a complex factor or potentially solve a problem.

Here are the examples from above shown in one PR:

> *Minimal distractions from task engagement: To foster the development of expertise, minimal distractions from deep engagement with the work and problem space is important. Distractions reduce the time available to work on problems. Ineffective meetings are considered a distraction.*

In each PR, we included only those grammatical elements supported by the raw data: We did not infer any of them. Some PRs were not written with this grammatical structure because they reflect two additional kinds of interview data collected: higher order thinking skill (HOTS) data and rating data. Some of the raw data we collected reflect HOTS requirements of experts. In past research, HOTS data were grouped into eight levels of the Bloom's taxonomic structure [Anderson 2001] to reflect eight levels of HOTSs. Raw data points from a variety of participants reflecting different HOTS levels were aggregated into a single PR: one PR for each of the eight levels. The PRs written from ratings data provide the summary statistics for all 10 participants in each PR.

3.2 Analysis Results

PRs were categorized into those with respect to experts, novices, teams, organizations, and cognitive abilities. We then grouped these categorized PRs into high-level (more generic) and low-level PRs (more specific). We also created a separate category for cognitive ability PRs (e.g., memory capacity, mathematical reasoning skills). This section begins with a brief discussion of the emergent milestones in the development of expertise, followed by a discussion of the high- and low-level PRs, and finally, the cognitive ability PRs generated. The results of this research are grounded in the raw data generated in our interviews. Each statement made by each participant was labeled with the following comment number format: "(P9-16)," denoting participant P9's comment #16 in P9's transcript. The results generated in this analysis by the researchers are often referenced directly back to the underlying raw data via the comment number.

Emergent Milestones. Developing expertise in malicious-code reverse engineering may initially involve a series of sequential milestones achieved by novices on their way to reaching a certain intermediate level of expertise (milestones 1-3). Once this intermediate level is reached, the development from intermediate to expert status was reportedly achieved though significant amounts of time spent in high-quality task engagement (milestones 4-5). The length of time required to achieve each milestone is an individual difference, yet we report estimates provided by study participants. All comments attributed to the comment numbers provided in this paragraph are listed in Table 4 below. The first milestone is achieved when novices learn proficiency in the IDA Pro disassembler, compilers, debuggers, and other job relevant software (B1-7). The second milestone occurs at approximately 8-12 months post-hiring when novices become "operational" as indicated by a significant reduction in the amount of assistance required to execute daily task work (B1-9). The third milestone occurs when the junior reverse engineer's knowledge about a problem-solution space is comparable to the expert's level of knowledge. This occurs when the more junior engineer has attempted all strategies an expert would attempt but without the guidance of an expert. When the two meet to discuss the problem-solution space and the expert cannot offer a strategy that the junior engineer has not already attempted, this junior engineer has reached this third milestone (P9-22, P9-25, P11-11). The fourth milestone occurs with some type of organizational promotion to a senior reverse engineering job, approximately five to seven years post-hire (P4-3). The final milestone is not easily discernible but occurs with repeated difficult challenges that are

solved without the assistance of another reverse engineer; fellow reverse engineers do not have the knowledge/skills to provide assistance on these challenges. Thus, this fifth milestone is characterized by repeated experiences in which the reverse engineer must persist through his or her own ignorance (P11-11). Study participants identified the fifth milestone as an indication of an expert.

High- and Low-Level PRs. PRs are grouped according to how much detail they contain. Those with more detail (high-level PRs) are reviewed first below, followed by those with less detail (low-level PRs). The high-level PRs are about expert, novice, team, and organizational required attributes. The low-level PRs are about required knowledge, cognitive skills, and cognitive abilities for malicious-code reverse engineering experts.

Appendix A contains a table of all the expert, novice, team, and organizational high-level PRs generated from these interviews. A *novice* in this analysis is defined as any person who has little or no experience reverse engineering in an organizational setting. Novice PRs reflect individual characteristics of new hires that indicate great potential for developing expertise rapidly. An *expert* is a master-level reverse engineer (i.e., someone who has reached milestone 5 and beyond), and respective PRs indicate individual attributes of these experts.

Only the high-level PRs (more generic PRs) are listed in Appendix A. The process of generating Appendix A is as follows. Because many study participants offered conceptually similar statements, we generated a single statement that reflected each concept and then created a link to the supportive raw data statements made by each participant. Given the space constraints, we did not list the supportive raw data statements; rather, we just included the respective comment number (for example, [P9-16]) in the participant's transcripts. Then, these single conceptual statements and respective comment numbers were grouped together based on a common theme in Appendix B. One common theme is captured on a single slide in Appendix B, and the supportive conceptual statement and respective supportive comment numbers are listed in each row of the table embedded in each slide. (Data that is proprietary has been omitted.) We then generated a single statement that captured this common theme, called a PR, and provided that PR at the top of each slide. In Appendix A, we listed these slide-based PRs, which are high-level PRs because of their generic nature, with the respective slide number. We then grouped the PRs into four types: (1) novice (individual), (2) expert (individual), (3) team, and (4) organizational. These high-level PRs describe observable attributes or qualities of each of these four entities. For example, the "expert" PRs not only assist in the identification of experts but also characterize attributes of their work experience. The boundary between team and organizational PRs is not distinct, so we define it here for research purposes. PRs pertaining to work attributes that are managed by Human Resources department staff (e.g., job descriptions, staffing requirements), management attributes above the team-lead level, and characteristics of the organization that directly impact the individual are all included under "organizational." Team PRs pertain to team dynamics (i.e., communication, work flow, decision making), team structure, and leadership. In sum, 18 PRs were written for novice requirements, 14 PRs for expert requirements, 10 PRs for team requirements, and 16 PRs for organizational requirements. Two PRs were redundantly classified as both team and organizational requirements.

Low-level PRs (more detailed PRs) involve individual knowledge and cognitive skills, with greater detail than high-level PRs. We include supportive comment numbers in this paragraph about low-level PRs but the raw data statements attributed to these comments are not included because the level of detail below is synonymous with the level in the transcript. The low-level PRs detail required analytic techniques as well as the types of knowledge experts required for stellar job performance. Analytic technique requirements include static and dynamic analysis, although it is not clear whether experts need to be highly skilled at executing and interpreting the results from both types of analyses. Experts are said to be strong at executing one or the other but not both. One participant opined that experts are often more knowledgeable at static analysis (P2-31) than dynamic analysis. In addition, experts must have a knowledge of various assembly instructions (P2-48, P4-11) including the most uncommon and common[10] aspects of them (P8-54). Experts need to identify patterns in the assembly code (P4-11) and transfer the high-level interaction knowledge over to a different architecture. For example, they should be familiar with Intel Windows Platforms and the X86 assembly, including the 1700 assembly instructions as well as the more *interesting* assembly instructions[11] that are not used at a high level (P8-54).[12] Also, experts should be able to transfer their knowledge of assembly languages to mobile platforms (P8-54). In addition to assembly languages, experts have a diverse knowledge of various coding languages and high-level programming language constructs (e.g., object-oriented programming) (P2-48). This includes knowledge of how to write kernel drivers—an indication of a deep level of technical expertise (P2-48). Finally, knowledge of architectural internals, operating systems, executable formats, cryptography, and network protocols is indicative of high levels of expertise (P2-48). Because this research involves a study of a single team of reverse engineers, we expect this information to be incomplete and to be embellished with additional studies of other malicious-code reverse engineering teams.

Cognitive Ability PRs. Cognitive ability PRs are not necessarily observable individual characteristics that participants directly identified. Therefore, these PRs were inferred by the research team from the raw data collected. These were cognitive abilities that participants indicated experts possessed but since cognitive abilities are inherited and fairly stable individual traits, novices may also possess them. No standardized list of cognitive abilities and respective, agreed-upon definitions exist in the academic community, but O*Net publishes an open-source standardized list of four types of abilities that will be used here: cognitive, psychomotor, sensory, and physical. For this research effort, we selected abilities representative of these four types on O*Net and aggregated them to the generic PRs listed in Table 3. Each cognitive ability is listed in the table as a

---

[10] *Common* and *uncommon* refer to the arcana of instruction implementation. Examples of common aspects involve understanding how instructions manipulate the stack, flags, and so on, while uncommon aspects might involve understanding the interaction between processor state and the operating system running on top, undocumented instructions, and so forth.

[11] *Interesting* instructions are those whose effects on a program or machine state are not necessarily or immediately obvious, or those that are not used frequently (due to either disuse by compilers or handwritten assembly).

[12] *High level* refers to how reverse engineers identify and communicate the semantics and abstractions present in a bit of code. For example, some bit of malicious code might be copying its configuration into memory. A high-level summary might be "duplicating its config block," a medium-level summary might be "copying bytes from one memory location to another," while a low-level summary might be "copy using movsd/rep." It is important to understand what is going on at multiple levels of abstraction (i.e., the interesting aspects) so similar patterns of usage can be identified when the implementations are byte-for-byte different.

single PR. All cognitive abilities are defined, and next to each definition are the supporting raw data statement and the comment number in parenthesis. The supportive raw data is not exhaustive; we chose an exemplar or two to illustrate the required cognitive ability. Beyond the cognitive abilities listed in Table 3, working-memory capacity and long-term-memory capacity are also PRs that emerged from the collected data. The ability to hold *chunks* of information in working memory, retrieved from long-term-memory stores, while matching them to chunks of information perceived in the malware sample seems to indicate a need for large working-memory capacity. In addition, the ability to store large amounts of detailed information in long-term-memory stores to be retrieved at different frequencies intimates the requirement of a sophisticated long-term-memory encoding, storage, and retrieval capability.

Table 3: Potential Cognitive Abilities of Expert Malicious-Code Reverse Engineers Based on Raw Data

Cognitive Ability	Definition	Supporting Raw Data – Unedited (Reference)
Category flexibility	The ability to generate or use different sets of rules for combining or grouping things in different ways	Finding the clever aspects of code the hacker used is very interesting. Especially if there is nothing in the documentation that could help him (P4-49). Experts will sometimes look at encryption strategies [in the malware] and determine whether they've seen this type of encryption. If not, they are able to tell whether they need to investigate the encryption further (P8-35).
Deductive reasoning	The ability to apply general rules to specific problems to produce answers that make sense	There is some pleasure you get from writing [code] that survives one particular problem. There is a certain amount of excitement you get when something works outside of the thing you originally started with (e.g., writing a script that works across malicious code). ["Scripts" includes logic, rules, and knowledge the person learns over time] (P11-37). Pattern matching expertise is looking at the problem space and coming up with a list of patterns that you think will be important (P8-34). There are people on the team who argue that lower level languages like C and C++ are necessary but I don't care what language you know, if you can understand the basic constructs of programming language, you can apply it to any language (P4-54).
Flexibility of closure	The ability to identify or detect a known pattern (a figure, object, word, or sound) that is hidden in other distracting material	When you look at code, it's a bunch of bytes and you have to determine what bytes are for assembly instructions (called code) and what are data. No automated tools get the distinction between assembly instructions and data completely right so humans have to double check (P2-18). Sometimes experts pick out functions or sub portions of functions because this is a more difficult task. It's often a trial and error game. Experts can look at the choices and based on familiarity, they can choose what is more likely to produce good signal than other choices (P8-36).
Fluency of ideas	The ability to come up with a number of ideas about a topic	If they can recall the instance of an example pattern vs. having familiarity: depends on number of

Cognitive Ability	Definition	Supporting Raw Data – Unedited (Reference)
	(the number of ideas is important, not their quality, correctness, or creativity)	exposures, temporal distance, some people have a memory for everything they've ever worked on (P8-39).
Inductive reasoning	The ability to combine pieces of information to form general rules or conclusions (includes finding a relationship among seemingly unrelated events)	Experts often improvise through problem solving. They look at all of the facts and find patterns. They create new information by synthesizing the data and inferring new information from it (P1-15). The learning curve is extraordinarily high, things will be very confusing, and you need to systematically break down what you learn into chunks and be able to assemble those chunks as you go along (P4-55).
Information ordering	The ability to arrange things or actions in a certain order or pattern according to a specific rule or set of rules (e.g., patterns of numbers, letters, words, pictures, mathematical operations)	You have to hold a lot of details in your mind at the same time to be an expert and develop an abstraction that accounts for all of them and that abstraction can change in the face of new information. You have to have a detailed stack and rearrange the stack while staring at some bits (P11-22).
Mathematical reasoning	The ability to choose the right mathematical methods or formulas to solve a problem	Topics of knowledge required for expertise = math; different shifts, powers, multiplication and division. Need to go between base 10 and base 16 small conversions in your head (B1-103). Trying to teach someone reverse engineering when they don't even have a background in programming is very difficult (P9-17).
Memorization	The ability to remember information such as words, numbers, pictures, and procedures	He built up a lot of patterns that he could recognize in his memory for what it is and what it does and he could take those patterns he identified and assimilate them together to paint the picture for what malware was doing. This was based on lots of experience analyzing malware (P4-31). If they can recall the instance of an example pattern vs. having familiarity: depends on number of exposures, temporal distance, some people have a memory for everything they've ever worked on (P8-39).
Near vision	The ability to see details at close range (within a few feet of the observer)	We look at the raw assembly code and we see what the machine would process (P4-11).
Number facility	The ability to add, subtract, multiply, or divide quickly and correctly	Topics of knowledge required for expertise = math; different shifts, powers, multiplication and division. Need to go between base 10 and base 16 small conversions in your head (B1-103).
Oral expression	The ability to communicate information and ideas in speaking so others will understand	When at a conference and I'm watching a presenter, good reverse engineers don't gloss over the technical details. They might go deeper in the middle but begin to hand wave at the end of the presentation, that's a cue that they are not prepared to go into lots of detail. Also Q & A must be detailed (P2-23).

Cognitive Ability	Definition	Supporting Raw Data – Unedited (Reference)
Originality	The ability to come up with unusual or clever ideas about a given topic or situation, or to develop creative ways to solve a problem	Expertise involves having a variety of approaches to solving a problem in their head (P2-42). The job is very intellectually taxing, you have to have some creativity (P11-23).
Perceptual speed	The ability to quickly and accurately compare similarities and differences among sets of letters, numbers, objects, pictures, or patterns. The things to be compared may be presented at the same time or one after the other. This ability also includes comparing a presented object with a remembered object.	If they can recognize patterns they've seen before, they cut down on the time they need to look at something. You need to speed up the process (P9-18).
Problem sensitivity	The ability to tell when something is wrong or is likely to go wrong. It does not involve solving the problem, only recognizing there is a problem.	When doing obfuscation work, the code is often scrambled in a way that is different every time. It's very hard to pick out the signal from the noise and an expert can find patterns in this obfuscation which is extremely difficult. Also the expert knows when to stop doing the analysis because he knows that he's not going to find a signal there across all the noise (P8-32).
Selective attention	The ability to concentrate on a task over a period of time without being distracted	A variety of work is not important because distractions are the killer. Context switching has adverse consequences because you cannot reach the depth you need. Novices who don't context switch all the time have the greatest chance of becoming successful (P11-50).
Speed of closure	The ability to quickly make sense of, combine, and organize information into meaningful patterns	Good reverse engineers are advanced at pattern recognition. When you make those connections within one code and across different codes; it's okay if you don't know what the patterns mean, it's that you see the pattern (P2-17). The experts look at [a challenge problem] and give the answer instantly because they've seen similar stuff like this before. The novices cannot get through it quickly (P8-13).
Time sharing	The ability to shift back and forth between two or more activities or sources of information (such as speech, sounds, touch, or other sources)	[Observed behavior]
Visual color discrimination	The ability to match or detect differences between colors, including shades of color and brightness	Workers even name functions in IDA with various names that made sense to them and what makes sense to them won't make sense to anyone else. [Some naming conventions and respective semantics are color coded in IDA and these are quickly reviewed by the reverse engineer to create patterns of color to represent semantic patterns] (P2-

Cognitive Ability	Definition	Supporting Raw Data – Unedited (Reference)
		27).
Visualization	The ability to imagine how something will look after it is moved around or when its parts are moved or rearranged	You have to hold a lot of details in your mind at the same time to be an expert and develop an abstraction that accounts for all of them and that abstraction can change in the face of new information. You have to have a detailed stack and rearrange the stack while staring at some bits (P11-22).
Written comprehension	The ability to read and understand information and ideas presented in writing	Experts have inquisitiveness, the ability to abstract based on what they learn, the ability to restate problems in a way that educates the reader who is not as skilled as the reverse engineer stating them. Communication is a vastly underrated skill in this field. The depth of knowledge doesn't matter if you cannot get it across to an arbitrary audience (P11-20).
Written expression	The ability to communicate information and ideas in writing so others will understand	One [expert] he knew wrote fantastic work. The characteristics of good quality work were: 1. The report was a narrative which was important because technical reports can be very dry. He could tell the story of the malware as it was happening; not just describe what it was doing but trying to imagine why the author did what he did and what it gained them by doing it that way. He could write for the perspective audience by putting himself in the audience's shoes so you could tell if he was writing it for network defense or intelligence (P10-12).

Table 4: Raw Data from Participant Interviews

Participant	Raw Data (Unedited)
B1-7	I didn't do reverse engineering at first; just liaison with customers and getting familiar with it and the tools. I was entry level and transitioning to malware analyst
B1-9	To plateau to operational status, it takes one year of daily practice. Plateau is 80% productivity.
P2-31	People can be an expert at either static or dynamic analysis. They tend to be good at only one of the two. I am a great static guy; I have poor runtime skills. If you don't know how to do static analysis, you're screwed.
P2-48	[Knowledge requirements:] Assembly language, architecture internals (how to write a kernel driver), operating systems, executable formats, network protocols (packet headers and check sums level of knowledge [he goes into much detail here], high level programming language constructs (e.g., object oriented programming), a variety of languages, crypto
P4-3	It takes five years of experience to get to senior.
P4-11	We look at the raw assembly code and we see what the machine would process. There are patterns in there and there are ways the computer does things that you learn over time. Experienced people can see those patterns and reason through them quickly and a novice takes time to figure that out.
P8-54	For expert, they need a moderately detailed knowledge of the most common and several of the uncommon aspects of the various assembly languages. They also need to transfer the high level interaction knowledge over to the architecture as appropriate. For example, they should know Intel Windows Platforms, knowledge of X86 assembly, including of the 1700 assembly instructions, the more interesting assembly instructions that aren't used at a high level. And an intimate knowledge of the most frequently occurring assembly instructions. And the ability to transfer that onto the mobile platforms for example. Understanding how it works on this new platform.
P9-22	[an example critical incident] years and years ago…..there was a person in the office that you would go to when you had a problem. He would sit in his cubical, he would listen to thumping dance music, and he would say, "yes, do this" and sure enough that would fix the problem. After repeated visits to this person over time on different problems, you'd get to the point where you'd already try his first suggestion before he told you. Then one day, I brought a problem to him and I told him that these are the things I've done and it still doesn't work and he would say, "that's very strange. I don't know what you should to. I've never had this happen before. You're going to have to figure this one out." Then, once you figure it out, you go and share that with this experts.
P9-24	The novices think that there is someone on the team who knows everything and I'm not as smart as him. But fortunately, it doesn't take too long before the novice outstrips the expert.
P9-25	That's a huge point when the novices have become a peer with the experts.
P11-11	To get to a pretty senior level of knowledge, you need a minimum of 5 years of experience. You need to go through a significant number of challenges that you cannot get help and still be required to solve the problem. You learn your own limitations in those circumstances and how to overcome them. Thus, the work and the task are not daunting, you just need to work through your ignorance.

4 Conclusions and Key Insights for Stakeholders

In sum, this malicious-code reverse engineering job role is about the development of experts and masters. Without rapid development of high levels of expertise, the task work becomes exhausting, and consequently the retention of new hires suffers.

Research on expertise development indicates that across many domains, *quality time on task* is the most important predictor of expertise development [Clark 2008, p. 202], which many participant comments supported. Quality time on task, called *deliberate practice* [Ericsson 2006], is defined as the diligent focus on mastering key work aspects through an expertise development process with the end goal of improving overall performance. Participants mentioned that the most senior experts were typically older and had many years of repeated experience handling difficult problems. Distractions from daily task work seemed to prohibit the development of expertise. Thus, any activity stalling or prohibiting deliberate task engagement at the individual, team, and organizational levels may subsequently slow the development of expertise. And when the work becomes exhausting, reverse engineers are in danger of leaving the organization. Thus, it is important for individuals to structure their work in ways that maximize the amount of time spent being deeply engaged with the work. For such time structuring to become practice, the organization must encourage effective worker autonomy. Even though these individuals do most of the deep technical thinking in isolation, teamwork does exist through collaborative problem solving via joint malware analysis efforts. At the organizational level, inefficient and outdated policies and procedures that cover the access, analysis, and storage of malware samples can significantly slow the process of malware analysis and expertise development. In addition, the job role design outlined by Human Resources departments should be designed to maximize time on task by reducing or eliminating distracting job-related functions outside the purview of reverse engineering expertise (e.g., business development, administrative work, budgeting).

Several insights emerged that are important to stakeholders in training and curriculum development, and operations management. Training and curriculum development may only be possible for the training of entry-level individuals up to perhaps the first two milestones outlined in the "Analysis Results" section because of the vast amount of knowledge required for experts. Expertise in this domain does not necessarily entail the development of detailed knowledge and skills on a few topics; it is about developing sufficient breadth of skills and knowledge on computer software and hardware to enable finding the information needed to understand how the malware impacts the hardware, software, and respective network. In addition, knowledge built from repeated experiences analyzing malicious code enables expeditious problem solving, which is especially important for time-sensitive sponsor-driven work. Many participants indicated that having at least a bachelor's degree in computer science will provide a well-rounded education, but, since much of the advanced knowledge is self-taught, the college degree is not mandatory and is not as important as having the motivation to learn new in-depth information. Teaching novices how to motivate themselves and how to become self-teachers may prove difficult for traditional training paradigms. Also, experts apparently have cognitive abilities (e.g., perceptual speed, deductive reasoning) that, according to theories of general intelligence, are not teachable.

There are also several emergent insights for organizational operations. First, severe job shortages of critical job roles like malicious-code reverse engineering require due diligence to attract, develop, and retain talent. Participants mentioned that an organization's team of reverse engineers is only as skilled as its senior-most reverse engineer. Thus, retention of the best talent is crucial to the development of new talent. Retention is enhanced by removing barriers to quality time on task and by attracting challenging malicious code problems to solve. These study results intimate a relationship between certain organizational operations that inhibit or encumber expertise development (i.e., high work-distraction rate, lack of recognition for excellent work, lack of team visioning, misfit with organizational strategies and mission) and personnel attrition. Generally, teams of experts working together may be a rare phenomenon in the workforce, so more research is needed to understand how, if at all, these individuals function together within an organizational context. Historically, counterproductive organizational cultures, policies, and practices imposed on a workforce caused it to adapt to working in sub-optimal and sometimes more inefficient conditions. However, expert reverse engineers are naturally autonomous, critical thinkers who may not always tolerate working conditions that impede efficient and effective work output. Thus, organizations may need to re-evaluate whether such impositions are related enough to attrition to warrant a different management paradigm that supports the emergent culture and requirements of reverse engineers.

5 Limitations

A few limitations and respective insights exist for both academic researchers and operations. First, the explanation of what an expert is from the reverse engineer's perspective is vague. Often, participants described attributes of an expert (e.g., these people are good oral presenters, they write excellent reports), but they could not articulate exactly what expertise is and how it can be effectively measured. Consequently, it is unclear whether sensitive metrics can be established that truly distinguish novices, intermediates, and experts. Once some level of self-reliance can be achieved, individuals continue to develop their own expertise. This expertise is a self-chosen balance between breadth and depth of knowledge often based on their own interests as well as previous experiences with certain classes of malicious code. While a certain level of knowledge and skills is required at certain milestones in the development of expertise, it is unclear what knowledge and skill requirements exist at each milestone. For example, one of the milestones is indicated when the trainee no longer requires frequent assistance from others to perform basic job duties that may be related to a specific developed skill set. From a training perspective, this milestone can serve as a training goal. However, beyond the initial milestones, the measurement of knowledge and skills may be moot, not only because of this specialization but also because experts have other equally important attributes. Experts were identifiable through proxy attributes (e.g., good writers, good oral presenters), but good oral presenters could also be non-expert reverse engineers. In addition, expert reverse engineers could also be poor writers. So future research needs to understand with what reliability and to what degree these attributes indicate expertise.

A second limitation of this research is that our data may have a groupthink bias. Information and opinions collected in these interviews may reflect the group's consensus rather than an individual's. Group members for whatever reason choose to not generate, analyze, or believe alternative ideas contrary to the group's, and, consequently, group consensus is maintained. Groupthink bias may be present because participants admitted the high level of group sociability and many of the responses collected were identical across participants, leaving doubt that individuals developed unique ideas. Interviewees indicated that certain group members had been thinking about problems and solutions studied in our interview for several months prior and that solutions were often discussed at social gatherings with team members. For example, when asked what attributes indicate novice reverse engineers, several participants mentioned that novices are likely to tout their own mundane findings. However, there is no certainty that groupthink bias was actually present. The results of our research could reflect healthy group decision making where alternative ideas were presented by willing parties, and after much debate and discussion, the team came to a healthy consensus. Groupthink bias is typically an indicator of group dysfunction or team complacency, whereas healthy group decision making is not dysfunctional. Future validation studies on alternative samples of reverse engineers will help distinguish between the two.

Appendix A Potential Requirements

Type	Slide #	Statement
Novice Individual	9	Personality-like traits: These are the top six most important personality traits required for expertise in descending order: 1. Interest in solving problems, 2. Self-motivated, 3. Contentiousness, 4. Takes initiative and 5. Shows creativity and 6. Remains up to date on current job knowledge.
Novice Individual	10	Personality-like traits: Autonomy—the ability to choose the work and the work pacing is important but team strategist should be intimate with these choices to minimize work duplication.
Novice Individual	10	Personality-like traits: There are problems with freedom to choose malware to work on because you may be duplicating someone else's work and not know it. [This is inefficient] [requirement=avoid duplication of work]
Novice Individual	12	Teamwork Skills: The new hire must have teamwork skills; e.g., the ability to overcoming team disagreements and the ability to coordinate with others to complete work. This is because reverse engineers acknowledge the need for teamwork skills. New hire selection criteria should include an assessment of the candidate's ability to overcome team disagreements.
Novice Individual	13	Teamwork Skills: These are the top five most important teamwork skills required for expertise development in descending order: 1. Ability to voice opinions freely, 2. Provide constructive performance feedback, 3. Welcomes new ideas, 4. Shares status information to improve team performance, 5. The ability to adapt with the team in dynamic environments. Also, team leadership job role should set boundaries for what acceptable team performance is.
Novice Individual	14	Gaming with the adversary: Create a work context in which some transparency exists between reverse engineer and adversary. Identifying and predicting the evolution of the adversary's skill attracts reverse engineers to this type of work.
Novice Individual	15	Attracted to smart people: Create teams that new hires perceive as intelligent because this has historically been known to attract new talent. Often this is because the person is hungry for knowledge.
Novice Individual	16	Not intimidated by hard work: Select new hires who are not intimidated by difficult and/or time-consuming problems because these tend to be successful hires. This is because experts constantly learn about their own ignorance and fear should not prohibit them from working through their ignorance.
Novice Individual	18	Domain-specific Knowledge and Skills: When selecting new hires, individuals who display depth and breadth of this domain-specific knowledge might help him/her become expert reverse engineers. Also, candidates need to demonstrate that they can converse on any topic (related or unrelated to computer science) to deep technical depths.
Novice Individual	19	Quick cognitive processing speed: New hire candidates who respond quickly to questions and challenge problems is a possible indicator of repeated experience with that type of problem. However, the response must be accurate. Processing speed is accrued with repeated exposure to problem set and a proxy indicator of expertise level.

Type	Slide #	Statement
Novice Individual	20	Meta awareness of problem space: Experts have the ability to build mental abstractions, (e.g., seeing the broader problems inherent in the discipline and seeing the nature of the problem he/she is currently working on) and new hires should have this ability as well. Since these types of abstractions are contingent upon prior work in the discipline, the ability to abstract is assessed through the quality of responses candidates provide to challenge problems. Thoughtful responses (e.g., pros and cons to each solution) that indicate the person's ability to articulate a broad perception of the problem and pros and cons to possible solutions instead of canned responses is important to personnel selection.
Novice Individual	21	Problem solving creativity: Select candidates on their ability to creatively solve problems. Some problems demand more out-of-the-box thinking so the selection of the candidate is based on the ability to reason through difficult problems.
Novice Individual	23	Educational degrees: There is no unanimous agreement about whether new hires should have earned at least a BS degree to be selected. Those who believe a BS degree is required believed the degree should be in any of the following: computer science, electrical engineering or computer engineering. Most reverse engineers believe that an advanced degree is not useful for reverse engineering.
Novice Individual	24	Certifications/Licensing: New hire candidates do not need certifications and/or licenses to verify their knowledge and skills.
Novice Individual	25	Prior work experience: New hire candidates should have work experience that provides knowledge and skills required for success. Most important is prior work experience as a reverse engineer or work involving malware, but other work experience as an incident responder, analyst position, system admin, software developer (e.g., also development in low level languages, C++, Delphi,) is also important. Also, work experience can be articulated by the types of problems worked on and/or the tools they developed.
Novice Individual	26	Prior research experience: New hire candidates who have conducted research projects in their work history may have some of the skills and knowledge requirements to be successful
Expert Individual	29	Conference attendance: The expertise of the new hires may be contingent upon the number and variety of security related conferences he/she has attended in the past.
Expert Individual	30	Work experience: Expertise is based on years of reverse engineering work experience that approximate "time on task." The more quality time the person engages with difficult reverse engineering challenges, the more apt to develop expertise. More experts new hire candidates may by indicated by their prior work experience in software development, writing system drivers and/or code libraries. Expertise seems to require 5 years minimum of reverse engineering experience which should include several difficult problems worked on without the assistance of others. This affords the repeated experience of working through their own ignorance; a possible requirement for developing expertise.
Expert Individual	32 and 33	Personality: Experts have an array of non-cognitive personality-like traits that may indicate expertise. According to the team, these traits are also visible in successful job candidates; these traits include persistence, passion for the work, openness to experience, minimally intimidated by problem solving, self-motivated, humility, curious, etc. In addition, tinkering, work-related obsessive compulsiveness, the ability to develop insights based on the work, and a bit of impulsiveness are also common traits of experts.

Type	Slide #	Statement
Expert Individual	34	Domain-specific knowledge and skills: Experts have both a breadth and depth of knowledge on a variety of hardware and software topics. The depth and breadth of the knowledge is driven by adversary's expertise. Part of domain-specific skills experts develop is the ability and motivation to create tools that assist in the automation of repetitive tasks. These tools are a reflection of the detailed knowledge and skills acquired over time in reverse engineering. In addition, the reverse engineer's level of expertise can be gauged by the difficulty of the problems being solved and the approach taken to solve them.
Expert Individual	36	Written communication skills: Expert reverse engineers tend to be highly skilled at technical writing and written correspondences; however, a poor writer does not indicate a poor reverse engineer. Writing quality is indicated by concise language describing abstract and complex phenomenon to less knowledgeable readership.
Expert Individual	37	Formal presentation skills: Experts are often skilled at formal oral presentations. Experts study their audience and communicate the relevant information in a way that facilitates understanding of deep technical knowledge. Experts also tend to be clear and concise oral communicators.
Expert Individual	39	Possesses 'remembering' higher order skill: Experts are able to quickly perceive and remember patterns of binaries based on past experience with these and other similar patterns. Patterns are not exclusive to binaries but can be, for example, patterns of assembly code instructions.
Expert Individual	40	Possesses 'remembering' higher order skill: The higher order thinking skills important to expertise is processing speed. The faster the person can recognize information and identify possible solutions, the more expert. Perceptual speed is contingent upon access to long-term memories of relevant information and working memory spans that accommodates perceived information in the environment, long-term memories, and other relevant information for decision making.
Expert Individual	41	Possesses 'understanding' higher order skill: Experts develop an understanding (through intuition or reasoning) for how malware works and why it works the way it does and what the adversary's intent was.
Expert Individual	42	Possesses 'applying' higher order skill: Experts apply learned knowledge and skills to assist in problem solving.
Expert Individual	43	Possesses 'analyzing' higher order skill: Expertise requires multifarious analytic capabilities. The person must be able to review a large amount of information and be able to use deductive reasoning, compare semantically different pieces of the code, and formulate an abstract mental model of how components of the malicious code interrelate
Expert Individual	44 and 45	Possesses 'evaluating' higher order skill: Experts demonstrate evaluation 1.) by judging what is fact and what is an unsupported assumption, 2.) by minimizing subjective options, and 3.) by being skeptical of results.
Expert Individual	46	Possesses 'creativity' higher order skill: Experts are creative; they have lateral and divergent thinking processes to generate an array of possible solutions to test.
Expert Individual	47	Possesses 'learning' higher order skill: Experts must be self-taught to fill in the knowledge and skill gaps that a piece of malicious code poses. This acquired information is from online sources, books, and colleagues.
Team	55	Appropriate work pacing: Time pressures and deadline-driven work is contrarian to productivity. Too much time pressure prevents individuals from having the time to think of new solutions and to think abstractly. Deadline-driven work makes it difficult to take the necessary to understand the malicious code at the depth required.

Type	Slide #	Statement
Team	58	Provide appropriate training: This position requires a formal mentoring program that implements a formal job training strategy because of the steep learning curve and autonomy. However, training expert skills and knowledge that are difficult to articulate poses a challenge. If the training includes tools, the emphasis should not be on the reliance of tools; rather on the value the tools provide and the meaning of the output.
Team	60	Enable Autonomy: This job role must be predominantly autonomous with the supportive management of the team leadership.
Team	62	Enable connection with the adversary: What attracts reverse engineers is the ability to understand the intent of the adversary and watch the adversarial capabilities evolve. This should be a required characteristic.
Team	64	Appropriate work tasking: Work should be determined by the sponsor's needs but should also fit with the overall team mission. Also, management should be familiar with individual work goals to maximize team efficiency.
Team	68	Team Structure: The team structure may need to be self-organizing; forming and dissolving based on the work type and on trusting interpersonal relationships.
Team	69	Fosters a culture of feedback and communication: Promote a culture of feedback and constructive communication. Performance feedback, both positive and negative, are important but too much unconstructive negative feedback can lead to lack of collaboration and attrition. Performance feedback is most important from the sponsors but perhaps equally as important from the organization and from peers.
Team	70	Advocate for the team to senior management: The team leadership (e.g., the team manager) needs to be an advocate for the team with respect to senior management. This leadership needs to convey the expertise and problem space the team works within such that senior management is aware of the value of the team and the value of the work.
Team	71	Enforces performance accountability: The team culture is that of highly accurate, high-quality deliverables. When performance is not positively and negatively reinforced, some team members produce subpar work quality, and this leads to friction and demoralization within the team. Ultimately, poor-quality work from a single individual reflects negatively on the entire team. Thus, quality work should be positively reinforced and poor-quality work, negatively reinforced from the formal leadership.
Team	72	Effective team leadership styles: Effective team leadership includes the ability to move between autocratic, democratic, consultative, participative, and laissez-faire leadership styles when appropriate. The leadership should have the ability to manage autonomous individuals, build team consensus, and also push the team to generate a team vision/mission/strategy that is overtly supported and articulated to senior management within the organization.
Team	73	Facilitate more intra-team collaboration and information sharing: Team collaboration and information sharing is a method to enhance the intellectual capital of the entire team. There are reasons why information sharing is difficult.
Organizational and Team	56	Minimal distractions from task engagement: To foster the development of expertise, minimal distractions from deep engagement with the work and problem space is important. Distractions reduce the time available to work on problems. Ineffective meetings are considered a distraction.
Organizational and Team	60	Autonomous job role: This job role must be predominantly autonomous with the supportive management of the team leadership.
Organizational	50	Create new job roles: Create a new job role for business development and funding solicitation for the team of reverse engineers.

Type	Slide #	Statement
Organizational	51	Hire new candidates: Adequately staff the team of reverse engineers.
Organizational	52	Modify existing job role: The malicious code reverse engineer job role needs to have the appropriate types of functional roles that reflect their expertise. For example, non-management reverse engineers should not have a business development functional role because this is outside of their expertise. The position should not have heavy role strain that would add temporal pressure and unnecessary distractions. Also, promotions should be based on goals and objectives that reflect their functional roles. Also, the funding paradigm with charge strings don't fit well with the nature of reverse engineering work so perhaps modify the funding paradigm to create a better fit.
Organizational	54	Work/life balance: The job should promote work-life balance demonstrated by having the flexibility to set work hours and to some extent, the work location (e.g., at the office or at home).
Organizational	57	Support the development of expertise: The job should be designed such that expertise development is not encumbered, rather supported. Not only does the development of expertise depend on "time on task" (see slide 31), but expertise is indicated by both speed and accuracy of deliverables. If either speed or accuracy is encumbered, friction occurs. Accuracy can be facilitated by collaborations across organizations to learn from other experts. Mentorship opportunities need to be provided to novice reverse engineers.
Organizational	59	Provide appropriate tools: This position requires tools for conducting daily task work (IDA pro, compiler, debugger, etc.), tools for storing and searching artifact catalogs, tools for customer access to reports, and tools that are generated by reverse engineers to automate work processes (e.g., malware decoding tools, de-obfuscation tools, etc.).
Organizational	61	Provide excellent work experience: The quality of the work experience must be high to reduce boredom and attrition. The work must be interesting, diverse, deeply challenging, and broadly impacting to attract and retain senior reverse engineers.
Organizational	63	Provide opportunities to watch adversary evolve: What attracts reverse engineers is the ability to understand the intent of the adversary and watch the adversarial capabilities evolve. This should be a required characteristic.
Organizational	65	Appropriate performance metrics: Create new performance metrics that accurately reflect speed and accuracy of work products. Do not use productivity metrics because they often are absent of indicators of quality. While deriving metrics that distinguish novices from experts is challenging, scenario-based metrics are suggested by reverse engineers.
Organizational	75	Create directorate mission that values malicious code reverse engineering: The organization needs to have a mission that includes the mission of the reverse engineering team. Without this, the team lacks fit with the organization and questions its value and importance to the organization. The team strategy should include a budget plan with a funding pipeline plan. The team strategy should also emphasize research (e.g. longitudinal analysis, trends analysis, etc.).
Organizational	77	Minimize attrition: This job role should minimize the following causal factors which have historically led to burnout and attrition listed below. These factors have been explicitly stated in the interviews to cause burnout and attrition.
Organizational	78	Groom and retain experts: The organization must devise a job role and work context environment that fosters the development and retention of experts.

Type	Slide #	Statement
Organizational	79	Value the team: The organization must overtly communicate the value of the team and their expertise they bring to the organization. Silence can be misinterpreted negatively and ultimately leads to team apathy, cynicism and demoralization.
Organizational	80	Create effective organizational senior management: Effective senior management creates an overall mission statement that reverse engineering fits into. Also, effective management tries to understand the nature of the reverse engineering work and team expertise, values and acknowledges the team expertise, removes boulders in the path to development of expertise, and creates a clear communication channel amongst reverse engineers, reverse engineering team leadership and senior management.
Organizational	81	Re-evaluate policies and procedures: The organizational policies and procedures that hinder the development of expertise stated on slide 2 must be re-addressed. Particularly, policies regarding release review, accessing malware in a secure environment, and storing and backing up copies of malware are policies that slow the work flow and deliverable rate to a frustrating degree.

Appendix B Raw Data from Interviews

Slide 9

Personality-like traits
(slide 1 of 2)

PR: These are the top six most important personality traits required for expertise in descending order: 1. Interest in solving problems, 2. Self-motivated, 3. Contentiousness, 4. Takes-initiative and 5. Shows creativity and 6. Remains up to date on current job knowledge.

Mean (*n*=6)	*SD*	Personality Dimension
96.67	8.16	interest in solving problems
90.83	9.17	Self-motivated
90.83	11.14	contientiousness
89.17	12.42	Takes initiative
86.67	15.06	Shows creativity
82.50	10.37	Remains up to date on current job knowledge
78.33	22.73	Obsessiveness (persistent, rumination, often inducing an anxious state)
72.50	37.38	Perfectionism
65.00	33.32	self confident
64.17	15.63	self esteem (an individual's sense of value or worth, or the extend to which a person values, approves of, appreciates or likes him or herself)
62.50	19.43	openness to experience (having wide interest, being imaginative and insightful)
53.33	34.59	Is calm and self accepting
53.33	39.83	novelty seeking (impulsive, exploratory, fickle, excitable, extravagant)
52.50	31.26	Is perceptive, tactful and sensitive
50.83	32.47	social interaction
27.50	29.28	impulsive
26.67	13.29	Agreeableness (trusting, compliant, empathetic, sympathetic)
25.83	23.75	Extraversion (gregarious, projecting one's personality overtly)
22.50	16.96	Has a conforming personality
12.50	13.69	inability to express emotions
11.67	12.11	harm avoidance (a tendency towards shyness, being fearful and uncertain, tendency to worry)
9.17	18.00	Neuroticism (tendency to become emotional or upset)
9.17	12.42	Inability or unwillingness to constrain impulses
5.00	10.00	Rigidity (inflexibility, difficulty making transitions, adherence to set patterns)
0.00	0.00	Psychoticism (aggressive and interpersonal hostility)

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Personality-like traits

9

Slide 10

Personality-like traits
(slide 2 of 2)

PR: Autonomy-The ability to choose the work and the work pacing is important but team strategist should be intimate with these choices to minimize work duplication.

Category	Sub-category	Raw Data	Source
Autonomy	to choose work	freedom to study a variety of topics and develop new solutions	P11-26
Autonomy	to choose the malware I work on	I want to choose what malware to work on that is interesting to me because I'll be spending large amounts of time on it	P11-39
Autonomy	to not publish in academic journals		P2-73
Autonomy	from time constraints	no time constraints to explore problems.	P11-26
Autonomy	Conflict	There are problems with freedom to choose malware to work on because you may be duplicating someone else's work and not know it. [This is inefficient] [requirement=avoid duplication of work]	P10-70
Computer passion	For computers	passion for computers and who works with them in their free time	P9-43
Computer passion	For computers	tools they use and why	P10-30
Computer passion	For computers	type of computer system they have at home	P9-42
humility		ability to admit when they are wrong	P9-5

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Personality-like traits

10

Slide 12

Has teamwork skills
(slide 1 of 2)

PR: The new hire must have teamwork skills; e.g., the ability to overcoming team disagreements and the ability to coordinate with others to complete work. This is because reverse engineers acknowledge the need for teamwork skills. New hire selection criteria should include an assessment of the candidate's ability to overcome team disagreements.

Category	Sub-category	Raw Data	Source
Teamwork	Skilled at overcoming team disagreements	We ask interviewees how they overcome team disagreements.	P10-28
Teamwork	Coordinating with others	Experts are good at coordinating with others [to complete work]	Beta1-121
Teamwork		ability to deal with the team	P4-53

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Other >

12

Slide 13

Has teamwork skills
(slide 2 of 2)

PR: These are the top five most important teamwork skills required for expertise development in descending order: 1. Ability to voice opinions freely, 2. Provide constructive performance feedback, 3. Welcomes new ideas, 4. Shares status information to improve team performance, 5. The ability to adapt with the team in dynamic environments. Also, team leadership job role should set boundaries for what acceptable team performance is.

Mean (n=7)	SD	Team Dimension
86.43	14.06	The ability of a team member to voice opinions freely
85.71	10.58	Performance feedback is constructive
80.71	19.88	The ability of team members to welcome new ideas
79.29	10.97	Team members share status information to improve performance
78.86	9.08	Team adapts to dynamic environment
78.57	17.96	Team leadership sets boundaries for what acceptable team performance is
77.14	16.29	The team coordinates for effective team performance
73.57	19.09	Team members ensure that other team members understand communications
73.43	15.46	Clear communication is supported and encouraged
72.14	23.25	Team orientation or the person's awareness of self with regard to position, time, place and relationship within the team.
71.43	17.01	Team cohesion
70.71	15.66	The team proactively anticipates negative events that could arise in the future
70.00	25.66	Team leadership sets boundaries for what acceptable team behavior is
66.43	14.06	The team proactively strategizes tactics that address possible negative future events that may arise
64.29	21.30	Team sociability occurs on non-work related topics
59.29	18.58	Team back-up behavior
48.71	19.02	The team tries to establish group unanimity and agreements rather than appraising all counter alternatives that may disrupt group agreement

13

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Other >

Slide 14

Enjoys gaming relationship with the adversary

PR: Create a work context in which some transparency exists between reverse engineer and adversary. Identifying and predicting the evolution of the adversary's skill attracts reverse engineers to this type of work.

Category	Raw Data	Source
I enjoy gaming relationship with adversary		P1(2nd)-41, P2-85, P4-47, P10-18
Reasons why	finding the clever aspects of the code the hacker used is very interesting.	P4-49
Reasons why	I don't like being victimized or duped	P1-42,
Reasons why	psychology of the hack and the intent is very interesting	P4-48
Reasons why	intimacy with the thoughts of the hacker as a defender is exciting. You can see what the hackers are doing but anticipating their next move and being correct is exciting. Watching hackers evolve is also interesting.	P1-23
Reasons why	What draws you to this work? "It's a new puzzle every day and I enjoy that. People who write this stuff are actively trying to mess with me by making it more challenging. I don't have to be way better than them, I just have to be a little better than them. My knowledge evolves when the author's knowledge evolves and that cat and mouse game is enjoyable."	P10-17
Reasons why	The ability to "feel" what the author is intending is important and exciting to him. He looks for whether the author makes subtle changes in his code and that may help to profile the author. Are these subtle changes due to a mistake or intentional?	P1(2nd)-40
Reasons why	some get really excited by watching the adversary do their work. One person monitored communications between the bad guys in the underground	P2-84
Reasons why	finding mistakes in adversary's code is interesting	P4-35
Reasons why	when things go wrong on my computer and I know why, there's no secrets because I know why.	P4-44

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Other >

14

Slide 15

Attracted to working with smart people

PR: Create teams that new hires perceive as intelligent because this has historically been known to attract new talent. Often this is because the person is hungry for knowledge.

Category	Raw Data	Source
loves working with smart people		P1-44, P8-15
Reasons why	Novices and experts are hungry for knowledge	P8-19

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Other >

15

Slide 16

Not intimidated by hard work

PR: Select new hires who are not intimidated by difficult and/or time consuming problems because these tend to be successful hires. This is because experts constantly learn about their own ignorance and fear should not prohibit them from working through their ignorance.

Category	Raw Data	Source
Never intimidated by difficulties	If they think the problem is too hard, too daunting or going to take too much time to complete is a key indicator of poor candidate	P11-21
Do not fear ignorance	You are constantly learning more about your own ignorance as you advance; there are many more things you don't know that you do and you treat the new challenge with respect and not fear.	P11-16

Intra-Individual > Non-Experts New Hires > Psychology > Non-Cognitive > Other >

16

Slide 18

Domain-specific Knowledge and Skills

PR: When selecting new hires, individuals who display depth and breadth of this domain-specific knowledge might help him/her become expert reverse engineers. Also, candidates need to demonstrate that they can converse on any topic (related or unrelated to computer science) to deep technical depths.

Sub-Category	Raw Data	Source
Coursework topics	courses that teaches student advanced understanding of computer system	P7-17
	advanced security courses	P7-17
	a course that demonstrates why security is important	P7-17
	classes in IDA pro	P8-60
	classes demonstrating why applications and programs can be vulnerable	P7-17
	C and C++	P8-59
	assembly	P8-59, Beta1-116, P7-13
	java	P8-59
	.net technologies	P8-59
	low level architectures	Beta1-116
	computer architecture	P8-59, P10-33
	operating systems	P8-59, Beta1-116
	engineering	P10-33
	Systems design	P10-33
	Compiler design	P10-33
	software development	P10-33, P7-19
	programming classes involving different operating systems	Beta1-116
	Programming	P7-13
	Cryptography	P10-33, Beta1-116
	network classes	Beta1-116
	LINUX classes	Beta1-116
Depth of knowledge	Depth of knowledge must be deep on any topic	P2-52, P11-44

18

Intra-Individual > Non-Experts New Hires > Psychology > Cognitive >

Slide 19

Processing Speed

PR: New hire candidates who respond quickly to questions and challenge problems is a possible indicator of repeated experience with that type of problem. However, the response must be accurate. Processing speed is accrued with repeated exposure to problem set and a proxy indicator of expertise level.

Category	Raw Data	Source
speed of answering questions	this may indicate experience level if the response is correct	P7-13
speed of answering questions	novices cannot solve problems quickly.	P8-13

Intra-Individual > Non-Experts New Hires > Psychology > Cognitive >

19

Slide 20

Meta awareness of problem space

PR: Experts have the ability to build mental abstractions, (e.g., seeing the broader problems inherent in the discipline and seeing the nature of the problem he/she is currently working on) and new hires should have this ability as well. Since these types of abstractions are contingent upon prior work in the discipline, the ability to abstract is assessed through the quality of responses candidates provide to challenge problems. Thoughtful responses (e.g., pros and cons to each solution) that indicate the person's ability to articulate a broad perception of the problem and possible solutions instead of canned responses is important to personnel selection.

Category	Raw Data	Source
Identifying experts vs. novices	P10-32. I asked him how he would know that the person could think abstractly in an interview. He says asking open ended questions about challenges to the field. I like to ask questions about responsible disclosure of vulnerabilities for exploits. These types of topics are things you should be able to talk about for an hour if you have the depth. If the answers are too terse or canned, that's not good for abstraction. They need to demonstrate their reasoning and how they could see both sides. 38:10 in sum, they can see the big picture; drill down and then drill up on the details and come to no good conclusion.	P10-32
Identifying experts vs. novices	In an interview, he believes you can distinguish experts from novices. Here's how: They ask what the challenges of the field are. If they state things that are fairly trivial to solve, they're novice. If they are talking about things that are more 'pie in the sky' (because they know they exist) they are more experts and if they offer solutions, that means they've thoughts a great deal and are more senior. This is because first you have to know they exist. Then, they have to use their existing knowledge to come up with mechanisms to solve these problems	P9-40
Identifying experts vs. novices	Asking about challenges in reverse engineering in general and looking for specific answers to this question. Looking for indication that they can abstract away at their job: step back and see the bigger picture.	P10-28

Intra-Individual > Non-Experts New Hires > Psychology > Cognitive >

20

Slide 21

Problem Solving Strategy

PR: Select candidates on their ability to creatively solve problems. Some problems demand more out of the box thinking so the selection of the candidate is based on the ability to reason through difficult problems.

Category	Raw Data	Source
problem solving skills indicate level of expertise		
	creative problem solving skills are important to expertise. How well do candidates understand algorithmic complexity because this topic is harder and requires more out of the box thinking.	P8-20
	We give the candidate a description of malicious code and code's behavior and they ask the candidate to crack the code. When the candidate cannot do anything more, they ask for more information and then the interview team provides it. It's a matter of scaffolding the problem to see how the candidate solves problems.	P11-21, P8-13
	if we gave them a challenge problem, can they walk through their reasoning?	P7-13, P7-12
	Explaining the forward software development when presented with a software development problem in the interview	P7-19

Intra-Individual > Non-Experts New Hires > Psychology > Cognitive >

21

Slide 23

Degrees

PR: There is no unanimous agreement about whether new hires should have earned at least a BS degree to be selected. Those who believe a BS degree is required believed the degree should be in any of the following: Computer Science, Electrical Engineering or Computer Engineering. Most reverse engineers believe that an advanced degree is not useful for reverse engineering.

Category	Raw Data	Source
no degree required		P2-56, P2-57, P1-36, Beta1-36, P7-21, P10-31, P1-9, P4-24, Beta1-115, Beta1-115, P4-24, P2-47 (because they don't allow for depth)
BS Degree required in: Computer science, Electrical Engineering, Computer Engineering)		P7-20, P8-58, P4-25, P11-47
Degree is useful		P4-60, P11-42
coursework is not useful	Because it doesn't allow people to go into depth on a topic that is needed here	P2-47
Advance degree is not helpful		P3-12, P6-41, P11-47

Intra-Individual > Non-Experts New Hires > Experience >

23

Slide 24

Certifications/Licensing

PR: New hire candidates do not need certifications and/or licenses to verify their knowledge and skills.

Category	Raw Data	Source
Licensing required?	no	All participants

Intra-Individual > Non-Experts New Hires > Experience >

24

Slide 25

Prior Operational Work Experience

PR: New hire candidates should have work experience that provides knowledge and skills required for success.. Most important is prior work experience as a reverse engineer or work involving malware but other work experience as an incident responder, analyst position, system admin, software developer (e.g., also development in low level languages, C++, Delphi,) is also important. Also, work experience can be articulated by the types of problems worked on and/or the tools they developed.

Category	Raw Data	Source
Reverse Engineering	People who do reverse engineering are already familiar with the challenges of the work and more likely to tolerate it	P7-19,
A job in another domain	working in the gaming industry	P1-
In a related job	incident response is helpful	P4-59
In a related job	employed as a system admin or in programming. Assembly programming is good	P2-50
In a related job	anyone who has worked with malware before	P6-40
In an event	competed in capture the flag events because these events often involve reverse engineering	P7-15
In a related job	analyst position	P7-19,
In a related job	advanced engineer	P7-19,
Programming	Related work experience important to new hires : Have they written software before? Architecture doesn't matter so much. It's about whether they wrote code. (e.g, wrote system drivers, code libraries).	P4-59
Programming	Proficient programmer in low level languages	P7-17
Programming languages	C++ and Delphi	P7-17
Programming	do they program?	P7-13
Problems they worked on	Tools written in the past-Anything about how they do their job is an indication of expertise; tools written to help with their job, etc.	P8-8

25

Intra-Individual > Non-Experts New Hires > Experience >

Slide 26

Prior Research Experience

PR: New hire candidates who have conducted research projects in their work history may have some of the skills and knowledge requirements to be successful.

Category	Raw Data	Source
past research projects		P7-17
Has a track record of research awards?		P2-13

Intra-Individual > Non-Experts New Hires > Experience >

26

Slide 29

Conference attendance

PR: The expertise of the new hires may be contingent upon the number and variety of security related conferences he/she has attended in the past.

Category	Sub-category Raw Data	Source
attendance to various computer related security conferences		P8-60

Intra-Individual > Experts > Experience >

29

Slide 30

Work Experience

PR: Expertise is based on years of reverse engineering work experience that approximate 'time on task.' The more quality time the person engages with difficult reverse engineering challenges, the more apt to develop expertise. More experts new hire candidates may by indicated by their prior work experience in software development, writing system drivers and/or code libraries. Expertise seems to require 5 years minimum of reverse engineering experience which should include several difficult problems worked on without the assistance of others. This affords the repeated experience of working through their own ignorance; a possible requirement for developing expertise.

Sub-category	Raw Data	Source
Time on task	5 years minimum to get to a senior level of knowledge	P11-11
Time on task	Must go through a significant number of challenges that you cannot get help on and yet still solve the problem to get to expert	P11-11
	must work through your own ignorance	P11-11
Time on task	The more number of years of experience the more senior	PBeta1-35
	The ability to write system drivers, code libraries, etc. indicates expert status	P4-59
Time on task	Experts spend a lot of time to find the right answers	P10-15, P4-2, P11-18, P11-11
Time on task	Age is an identify of expertise. Older reverse engineers typically spend more time in the profession so these tend to be more senior.	P4-23
Time on task	Experts are committed and dedicated to the work	P4-37, P4-36

Intra-Individual > Experts > Experience >

30

Slide 32

Personality (Slide 1 of 2)

PR: Experts have an array of non-cognitive personality-like traits that may indicate expertise. According to the team, these traits are also visible in successful job candidates; these traits include persistence, passion for the work, openness to experience, minimally intimidated by problem solving, self-motivated, humility, curious, etc.

Category	Raw Data	Source
Persistence		P4-53
Persistence	to excel in this field, you need persistence	P1-34
Persistence	experts don't give up trying to solve a problem	P9-5
Persistence	Experts give up weekends to fix a problem and don't finish until the work is done	P4-36
Not intimidated easily	Not intimidated by math (NO FEAR)	P4-53
Not intimidated easily	You are constantly learning more about your own ignorance as you advance; there are many more things you don't know that you do and you treat the new challenge with respect and not fear.	P11-16
Not intimidated easily	not intimidated or afraid of trying to solve the problem	P8-64
openness to experience	the best have openness to experience,	P4-64

Intra-Individual > Experts > Psychology > Non-Cognitive >

32

Slide 33

Personality (Slide 2 of 2)

PR: Experts have an array of non-cognitive traits that represent dimensions of personality. These traits are also apparently visible in job candidates and include such traits as tinkering, obsessive compulsiveness, insightfulness, and a bit of impulsiveness.

Category	Raw Data	Source
passionate for the work		P4-52, P1-12
passionate for the work	you listen for the passion they have for solving a problem. Are they digging to find things out? Are they hungry for knowledge?	P9-9
passionate for the work	you must have passion for your work and know you will get your butt kicked every day.	Beta1-119
passionate for the work	passion and trust are the most important skills above technical skillsets. Technical skills can be taught.	Beta1-136
tinkerer		P10-38
self-motivated		P4-52, P9-9, P1-12
OCD		P9-5
curious	they want to know how things work and why	P9-5
curious	are they asking questions when they solve a problem? Are they digging to find answers?	P9-9
curious		P11-48, P4-64, P10-16, P11-20
insightful		P4-64
the ability to develop and relay insights		P6-38
imaginative		P4-64
Impulsivity	having impulsiveness gets you a start on the problem and gets you excited but you must error check your ideas.	P6-50
Impulsivity	this can be good in this profession. You might have an idea forr what you want to explore as a part of the investigation which may or may not pay off. Being unafraid of doing something is a good thing.	P8-64
inflexibility	one of the best guys were really set in their ways but he was really good in his ways. I don't necessarily think that is an asset	P4-66
humility		P11-16
keeping important information quiet	The only reason it's important to be shy is that you'd be more likely to keep your mouth shut. That's not important to be skilled as a RE but to be able to keep sensitive material quiet.	P6-52

33

Intra-Individual > Experts > Psychology > Non-Cognitive >

Slide 34

Domain-Specific Knowledge and Skills

PR: Experts have both a breadth and depth of knowledge on a variety of hardware and software topics. The depth and breadth of the knowledge is driven by adversary's expertise. Part of domain-specific skills experts develop is the ability and motivation to create tools that assist in the automation of repetitive tasks. These tools are a reflection of the detailed knowledge and skills acquired over time in reverse engineering. In addition, the reverse engineer's level of expertise can be gaged by the difficulty of the problems being solved and the approach taken to solve them.

Category	Raw Data	Source
breadth of knowledge	Attackers are extremely advanced and so you need a large foundation of knowledge to be able to study malware.	P1-34
breadth of knowledge	Experts use a diverse set of skills and knowledge in both hardware and software	P8-18
depth of knowledge	an expert has depth of knowledge; especially abstract concepts like computer architecture or how operating systems work or programming concepts.	P10-7
Tool building	Tools are built to execute tasks done repeatedly.	P9-41, P9-13
Tool building	Automating repetitive tasks	Beta1-112
Building knowledge and skills	Comes from working on past difficult problems	P8-9
Identifying knowledge and skills of experts	If they talk about some of the samples they tried to reverse engineer in the past, you can gage the quality of their work based on their description of the difficult problems and how they approached them	P8-9

Intra-Individual > Experts > Psychology > Cognitive >

34

Slide 36

Written Communication Skills

PR: Expert reverse engineers tend to be highly skilled at technical writing and written correspondences; however, a poor writer does not indicate a poor reverse engineer. Writing quality is indicated by concise language describing abstract and complex phenomenon to less knowledgeable readership.

Category	Raw Data	Source
Written communication	They have the ability to restate problems in a way that educates the reader who is not skilled. Communication is vastly underrated in this field. The depth of knowledge you have doesn't matter if it cannot be communicated to an arbitrary audience.	P11-20
Paper writing skills	Experts have the ability to write	P4-53, P10-14
Paper writing skills	Knowing how to frame the argument such that it appears important and explaining how these results impact the bottom line is useful. Also, being able to explain what this work is going to do for R&D and stakeholders is important in the writing	Beta1-108
Paper writing skills	A report with a high level of meticulous detail indicates that the report is likely to be accurate. And I am more likely to trust these results.	P1-21
Paper writing skills	You must know how to tell the people about your work or what's the point. Experts can communicate in a way that the person who didn't do the work can understand. However, there are experts who cannot write.	P4-57
Paper writing skills	Succinct statements of malware's capability with detailed mature language is important. Precise communication of the characteristics of the malware parameters.	P3-39
Paper writing skills	Experts consistently use complex language; it gives you insights into the depth of their expertise on a topic.	P8-8
Paper writing skills	the ability to restate problems in a way that educates the reader	P11-20
Paper writing skills	A POOR WRITER DOES NOT MEAN THEY ARE A POOR REVERSE ENGINEER	P10-26, P4-57
Paper writing skills	High report quality is indicated by the topic; a topic that nobody knows about is high quality report	Beta1-51, P6-33
Paper writing skills	written clear communication is not about spelling correctly, it must convey the idea well	P3-67

36

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Communication >

Slide 37

Formal Presentation Skills

PR: Experts are often skilled at formal oral presentations. Experts study their audience and communicate the relevant information in a way that facilitates understanding of deep technical knowledge. Experts also tend to be clear and concise oral communicators.

Category	Raw Data	Source
Communication	Clear communication is strong communication. Clear communication should be a dialog, not a monologue.	P3-67
Presentation skills	Need to be confident	P6-46, P6-48
Presentation skills	Experts need to determine who the audience is and how to communicate the ideas well to them.	P6-32,
Presentation skills		Beta1-109, P8-12
Presentation skills	Good reverse engineers don't gloss over the details. Hand waving is an indication of the lack of detail. A detailed Q&A discussion is common with experts	P2-23
Presentation skills	Good presenters know what's relevant and don't present findings that duplicate someone else's work.	P6-33
Presentation skills	Content is good	P6-48

37

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Communication >

Slide 39

Remembering
(slide 1 of 2)

PR: Experts are able to quickly perceive and remember patterns of binaries based on past experience with these and other similar patterns. Patterns are not exclusive to binaries but can be for example, patterns of assembly code instructions.

Category	Source	Raw Data
Pattern recognition	P2-17	Good reverse engineers are advanced at pattern recognition (e.g., making connections within one code and applying it across different codes). It's okay if you don't know the meaning of the pattern, just that you see it.
Pattern recognition	P9-16, P4-33, P8-38	
Pattern recognition	P8-36	Sometimes experts pick out functions or sub portions of functions because this is a more difficult task. It's often a trial and error game. Experts can look at the choices and based on familiarity, they can choose what is more likely to produce good signal than other choices. We do this more here in this organization than others in the field.
Pattern recognition	P4-11	We look at the raw assembly code and we see what the machine would process. There are patterns in there and there are ways the computer does things that you learn over time. Experienced people can see those patterns and reason through them quickly and a novice takes time to figure that out.
Pattern recognition	Beta1-45	Experts can recognize a pattern with speed no matter how many variants of the theme exist.
Pattern recognition	P8-35	Experts will sometimes look at encryption strategies and determine whether they've seen this type of encryption. If not, they are able to tell whether they need to investigate the encryption used further
Pattern recognition	P8-36	look at choices in the signal/noise landscape and based on familiarity, produce signals.
Pattern recognition	P7-6	An expert can filter out noise and what is indicative of something important in the data that results from tool use. (e.g., IDA pro, disassembler, tracing, API hooks, etc.).
Pattern recognition	P4-31	He built up a lot of patterns that he could recognize in his memory for what it is and what it does and he could take those patterns he identified and assimilate them together to pain the picture for what the malware was doing.
Pattern recognition	P2-22	Sometimes assembly code is dummy code and often novices cannot discern this type of code. He elaborates. Certain modes (e.g., kernel mode) invalidates some assembly code making it false or filler code. He says, "In assembly code, something like 95% of all instructions come out of a set of about 10 or 15 instructions. And then there are like 600 additional instructions that you rarely ever see." So good reverse engineers become very familiar with what those 15 most common instructions are, what orders and patterns they appear in, and you know how the instructions behave. When they don't behave as expected, that cues that they are abnormal and probably not instructions.
Pattern recognition	P8-34	Looking at the problem space and coming up with a list of patterns that you think will be important.
Pattern recognition	P4-11	look for patterns in assembly code

39

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 40

Remembering
(slide 2 of 2)

PR: The higher order thinking skills important to expertise is processing speed. The faster the person can recognize information and identify possible solutions, the more expert. Perceptual speed is contingent upon access to long term memories of relevant information and working memory spans that accommodates perceived information in the environment, long term memories and other relevant information for decision making.

Category	Sub-category	Raw Data	Source
Perception	speed	Experts self select problems that they have experience in so they can finish work quickly	P2-44
Perception	Speed and accuracy	experts need to be both fast and accurate and nothing else.	P8-28
Perception	speed	fast at perceiving what to focus on in the problem space	P4-32
Perception	speed	experts see patterns in assembly code and reason through them fast	P4-11
Perception of	Functions and sub portions of functions	Experts pick these out because they are difficult	P8-36
Perception	long-term memory requirements	Tricky patterns in the past will stand out in the mind	P8-38
Perception	long-term memory requirements	Good reverse engineers keep track of the details meaning: there is a lot of stuff to write down and there is no way to say what you wrote down is meaningful and what is not meaningful until you wrote everything down and saw the pattern. So he says, "Until you have the insight, you generally don't write it down." So the details have to be kept in the head.	P2-16, P8-36, P2-17, P4-11, P8-35, P4-31, P8-38
Perception	long-term memory requirements	recalling an instance of a pattern they learned before. Some have a memory for everything they've worked on.	P8-39
Perception	long-term memory requirements	Have to hold a lot of information in your head	Beta1-60
Perception	long-term memory requirements	holding lots of details in mind at the same time and develop an abstraction that can change with new information,	P11-22
Perception	working memory requirements	You have to be able to have a detailed stack of information, arrange the stack while staring at some bits.	P11-22
Perception	working memory requirements	Have to hold a lot of information in your head	Beta1-60

40

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 41

Understanding

PR: Experts develop an understanding (through intuition or reasoning) for how malware works and why it works the way it does and what the adversary's intent was.

Raw Data	Source
it is not enough to know how things work, they want to know why things work	P9-5
understand why the attacker wrote the code	P4-33
Intuition is sometimes used by experts to understand the malicious code; this is an ability that does not rely on induction or deduction	P1-7
Understand the adversary (intentions, etc.)	P1-43

41

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 42


Applying
PR: Experts apply learned knowledge and skills to assist in problem solving.
Raw Data
Source
Experts know what to do once the unpacking has been done
P7-8
Expertise is gaged by knowing how to crack the malicious code to answer the sponsor's questions
P7-18
42
Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 43

Analyzing

PR: Expertise requires multifarious analytic capabilities. The person must be able to review a large amount of information and be able to use deductive reasoning, compare semantically different pieces of the code, and formulate an abstract mental model of how components of the malicious code interrelate to answer problems.

Category	Raw Data	Source
analytic capabilities		P7-18
Deduction and comparative analysis	The ability to develop and relay insights. Draw conclusions based on a lot of information. Deduction. Abstracting. Comparative analysis of semantically different but operationally the same program.	P6-38
Abstraction	An expert is not the person who knows a lot of information but who can understand how the details interrelate and can be manipulated to solve a particular problem. Not the nitty gritty details	P11-15
Abstraction	the ability to abstract based on what they learned	P11-20
Abstraction		P6-38, P11-22

43

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 44

Evaluating
(Slide 1 of 2)

PR: Experts demonstration evaluation by judging what is fact and what is an unsupported assumption, by minimizing subjective options, and by being skeptical of results.

Sub-category	Raw Data	Source
separates facts from assumptions	this distinguishes novice from experts. You'll spend a lot of time reading code and figure out what it does so you have to make sure you don't reach incorrect conclusions. In order to do this, you have to separate facts from assumptions. You have to be able to reason through complex puzzles and keep track of all the details. These are what differentiates good from poor Reverse engineers.	P2-14
separates facts from assumptions	In particular for good reverse engineers, it's frequently the ability to say, "I saw this thing in the code that doesn't really match with this explanation." And if you can remember that, and make that connection and go back to the code and see it, you can say that proves it that the assumption is incorrect.	P2-15
separates facts from assumptions	Experts only state what they know. Novices don't fully verify their work.	P6-12
separates facts from assumptions	Don't make attribution claims that cannot be supported	P3-42
separates facts from assumptions	experts don't jump to conclusions early on; especially if tedious code. They wait until their conclusions are fully supported	P8-31
separates facts from assumptions	Experts can recognize when their brains are taking short cuts that are built on assumptions to solving the problem	P4-34
separates facts from assumptions	The team saying is "Show me your bits or you're full of shit"	P6-13
separates facts from assumptions	assumptions can negatively impact the accuracy and quality of the work because they are often wrong	Beta1-49
separates facts from assumptions	sometimes we do make attribution claim that cannot be supported but you must say as an expert that you are making an unsupported claim that may be false t	P3-41
separates facts from assumptions	even if you sound intelligent, that is not enough. They want to know how the conclusions were drawn. Where did they get their information? They don't want to know what the findings are but how you know what you got is true and accurate.	P10-10
separates facts from assumptions	An expert can filter out noise and what is indicative of something important in the data that results from tool use. (e.g., IDA pro, disassembler, tracing, API hooks, etc.). it's pretty easy to jump the gun to sound the alarm when something might not always be bad (e.g., experts don't necessarily lead off of assumptions) so experts don't jump the gun.	P7-6

44

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 45

Evaluating
(Slide 2 of 2)

PR: (same as previous slide)

Category	Raw Data	Source
critical thinking	When listening to presentations or reading reports, experts want to know how you came up with the results you got and how you believe these results are true and accurate	P1-34, P10-10, P8-29
skepticism		P10-10
the ability to develop and relay insights		P6-38
The ability to draw conclusions based on a lot of information		P6-38
not opinionated or subjective		P6-12
Understand the adversary	Understanding how the attacker thinks	P7-16
Understand the adversary	must predict what the adversary will do next once they are on the machine.	Beta1-42,
Understand the adversary	you must find the intent	P4-20
Understand the adversary	understand what they are trying to do and how the code structure helps them do that.	Beta1-38, Beta1-43

45

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 46

Creating

PR: Experts are creative; they have lateral and divergent thinking processes to generate an array of possible solutions to test.

Category	Raw Data	Source
creativity		P11-23
divergent thinking	experts are revealed in the way they answer questions. They thought processes behind their answers indicates critical or out of the box thinking.	P8-29
divergent thinking	its good to think outside of the box and take risks to approach the work.	P8-64,
Have a variety of approaches to solving problems, based on repeated experiences with the problem space		P2-42, P2-40, P2-41, P4-10
Problem solving	If I cannot figure something out, I relax my brain to see if solutions pop up over time.	P4-129
lateral thinking		P1-34

46

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 47

Learning

PR: Experts must be self-taught to fill in the knowledge and skill gaps that a piece of malicious code poses. This acquired information is from online sources, books and colleagues.

Sub-category	Raw Data	Source
Acquisition	Must learn and recall new techniques to cracking malicious code along the way	P4-10
Acquisition	Once the same phenomenon is experienced repeatedly, he learns and leverages this knowledge for the next similar problem	Beta1-53
Finding information	Google, colleagues, books, online	P4-129, Beta1-120
Finding information	Finding info on a class of malicious code on the internet is not taken seriously	P2-64
Finding information	I do not use other people's reports for knowledge because you don't know what they left out of a report. No report tells you what has not been done	Beta1-63
speed	must learn what to ignore to reduce the problem space	P4-32
of patterns	good at pattern matching	P9-16
type of knowledge I need	driven by adversary	Beta1-118

47

Intra-Individual > Experts > Psychology > Cognitive > Non-Domain-Specific Knowledge and Skills > Higher Order Thinking Skills >

Slide 50


Create new roles
PR: Create a new job role for business development and funding solicitation for the team of reverse engineers.
Sub-category
Raw Data
Source
Proprietary data omitted
P7-39
50
Intra-Organizational > HR Job Role Definition >

Slide 51

Hire new candidates

PR: Adequately staff team of reverse engineers.

Category	Raw Data	Source
understaffing	We are severely understaffed.	P2-71, P11-46

51

Intra-Organizational > HR Job Role Definition >

Slide 52

Modify existing roles

PR: The malicious code reverse engineer job role needs to have the appropriate types of functional roles that reflect their expertise. For example, non-management reverse engineers should not have a business development functional role because this is outside of their expertise. The position should not have heavy role strain that would add temporal pressure and unnecessary distractions. Also, promotions should be based on goals and objectives that reflect their functional roles. Also, the funding paradigm with charge strings don't fit well with the nature of reverse engineering work so perhaps modify the funding paradigm to create a better fit.

Category	Raw Data	Source
role strain: Business Development	Don't add business development [to my taskwork]	P3-106
Role Strain: Acquiring knowledge	need time to prepare. You need time to prepare (knowledge building) for doing the work and that is not included in the work plans or funding paradigm	P4-124
Role Strain: Executing work for former job	I still do a little supportive work for the engineering team he used to work for. Some of that work is just a transitions problem; finishing up on work that was a part of his former job 1;11:30. It's not malware work; it's helping them while that other team beefs up their staff.	P7-41
Change promotional structure	Promotions should be achievements of items within a set of reasonable goals and objectives based on your existing job role.	P10-62, P10-63
charge string	Charge strings don't synch with workflow and task functions	P3-19, P3-85, P6-63, P4-122, P4-124

52

Intra-Organizational > HR Job Role Definition >

Slide 54

Work/Life balance

PR: The job should promote work-life balance demonstrated by having the flexibility to set work hours and to some extent, the work location (e.g., at the office or at home).

Raw Data	Source
Lack of time constraints on the work (e.g., deadline-driven work) is favorable to developing expertise.	P11-26
Flexible work hours is important	P4-74, P7-51, P10-52

54

Intra-Organizational > Job Attributes >

Slide 55

Appropriate Work Pacing

PR: Time pressures and deadline-driven work is contrarian to productivity. Too much time pressure prevents individuals from having the time to think of new solutions and to think abstractly. Deadline driven work makes it difficult to take the necessary to understand the malicious code at the depth required.

Category	Raw Data	Source
Do not enforce busy-ness	Do not have arbitrary task work that does not support the development of expertise	
	Too much time pressure does not allow the individual time to explore and find solutions to problems	P4-129, P9-45, P1(2nd)-1
	Having time to dislodge knowledge or find solutions to problems takes time. I go for a run, change tasks, etc. and eventually, I think of a new solution.	P4-129
	idle time lets you think abstractly	P10-61
	having the freedom to work on problems at my own pace to go into enough depth to get the right answer	P10-53
	give them one free day to explore problems a week	P10-42
To prevent busyness	you need to be able to block time in your schedule to do it	P3-82, P3-83
	Streamlining processes like condensing reports or referring to other written reports	Beta1-55, P2-65
	streamlining processes like unpacking	P6-26
	streamlining processes by collaborating or asking colleagues more for help	P2-37

55

Intra-Organizational > Job Attributes >

Slide 56

Minimal distractions from task engagement

PR: To foster the development of expertise, minimal distractions from deep engagement with the work and problem space is important. Distractions reduce the time available to work on problems. Ineffective meetings are considered a distraction.

Category	Raw Data	Source
Improve meeting effectiveness so it is not a distraction		
	Make them an open-floor format to discuss issues	P3-62
	Do not mix meetings with working group formats	P7-54
	Create effective working group meetings (e.g., do not make the team predominantly novices who slow down the pace of the meeting)	P10-41, Beta1-71, Beta1-74, Beta1-84, P9-76, Beta1-69, P9-77, P4-127
	Make them more than once a month; if not, people meet anyways	P7-52, P7-56
	Reduce the number of standing meetings for leadership positions	P3-74, P7-56
	make people show up on time, reduce side conversations, provide an agenda ahead of the meeting.	Beta1-122
Reasons for minimal distractions from task engagement	Reverse engineers have a job requirement for solitude to engage in the work. When you are in a team structure, it must facilitate solitude. When the team is exposed to chaos and distractions from the organization, you won't' be successful and this is the case here in this organization.	P11-70
	Those who are distracted, are more junior	P11-84

56

Intra-Organizational > Job Attributes >

Slide 57

Supports the development of expertise

PR: The job should be designed such that expertise development is not encumbered, rather supported. Not only does the development of expertise depend on "time on task (See slide 31), but expertise is indicated by both speed and accuracy of deliverables. If either speed or accuracy is encumbered, friction occurs. Accuracy can be facilitated by collaborations across organizations to learn from other experts. Mentorship opportunities need to be provided to novice reverse engineers.

Category	Raw Data	Source
provide an environment where speed and accuracy of deliverables are supported.	Allow effective working groups to form within the organization and external to the organization. Very few reverse engineers exist so collaboration historically has been effective at solving problems quickly and accurately. But the organization must figure out a way to share techniques and tactics across organizational boundaries. who may or may not be competitors.	P10-41, Beta1-71, Beta1-74, Beta1-84, P9-76, Beta1-69, P9-77, P4-127, P11-70
Collaborations	Through collaborations external to the organization to facilitate knowledge exchange	
Mentorship opportunities		Beta1-11, Beta1-10

57

Intra-Organizational > Job Attributes >

Slide 58

Training

PR: This position requires a formal mentoring program that implements a formal job training strategy because of the steep learning curve and autonomy. However, training expert skills and knowledge that are difficult to articulate poses a challenge. If the training includes tools, the emphasis should not be on the reliance of tools; rather on the value the tools provide and the meaning of the output.

Category	Raw Data	Source
Reasons why	need mentoring and collaboration for new hires to provide structure	P4-80, P11-67
Reasons why	mentoring is needed because of the steep learning curve	P7-23
	need formal job training strategy	P10-34
What not to teach	don't teach textbooks because it doesn't work (too much materials to write in a book, limited guidance on what to do when something is wrong)	P10-8, P1-14, P1(2nd)-8
Problems with course content	hard to teach skills of experts because experts cannot articulate complex skills and strategies well	P2-39
Teaching subjects to be self-learners	Once training is complete, the rest of the training is self-motivated via trial and error	P10-35
Teaching tool output	make sure you teach what the output of the tools means.	P4-19, P2-19
Teaching tool value	Teach individuals the limited value of tools.	p4-18, p1(2nd)-17, P9-31,

58

Intra-Organizational > Job Attributes >

Slide 59

Tools

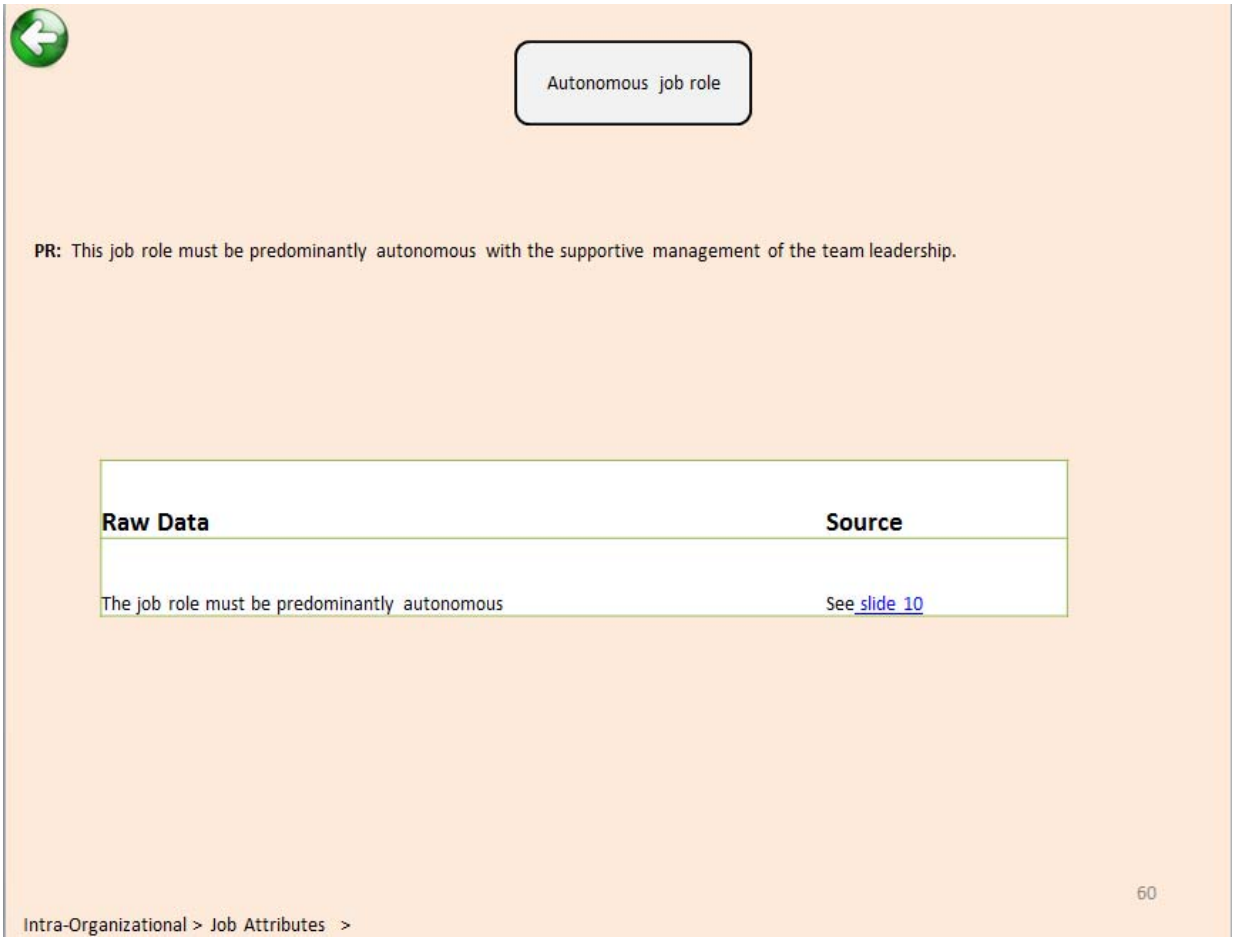
PR: This position requires tools for conducting daily task work (IDA pro, debugger, etc.), tools for storing and searching artifact catalogs (BigRep), tools for customer access to reports (i.e.,), and tools that are generated by reverse engineers to automate work processes (e.g., malware decoding tools, de-obfuscation tools, etc.).

Sub-category	Raw Data	Source
customer wants tools	tools for detecting similarities across different codes.	P2-60
customer wants tools	tools do to reverse engineering	P4-99
customer wants tools	code to help the customer decode the malware quickly	P4-93
customer wants tools	de-obfuscation programs...tool generates reprots based on similarities across malware that is difficult to detect with naked eye	P2-69
I use these tools on a daily basis	IDA pro	P1(2nd)-43, P1(2nd)-44,
Tools automate certain processes	we need to develop tools but not to automate the entire process but to help automate certain tasks in the process	P9-31
Problems	IDA pro does not search across different code	P4-105
Problems	BigRep (search engine in catalog) has poor search engine	P8-69
Problems	The artifact catalog should have a parameter that we can categorize the threat level of the malware	Beta1-59
Problems	they are not user friendly	P7-22
Problems	Tools don't always do taskwork perfectly so humans need to error check the tools. In addition, tools are difficult to devise to address complex problems. No automated tools get the distcintion between assembly code and data completely right so humans have to double check. My work is to get better tools to make distinctionb etween assembly instdcutions (called code) and data. New analysts have a hard time determine what's code and whats' data and with expertise, you just learn to tell. There are certain bites that are more common on code tahn data and he learns this over time with repeated experience.	P2-19, P2-18

59

Intra-Organizational > Job Attributes >

Slide 60


Autonomous job role
PR: This job role must be predominantly autonomous with the supportive management of the team leadership.
Raw Data
Source
The job role must be predominantly autonomous
See slide 10
60
Intra-Organizational > Job Attributes >

Slide 61

Provide excellent work experience

PR: The quality of the work experience must be high to reduce boredom and attrition. The work must be interesting, divers, deeply challenging, and broadly impacting to attract and retain senior reverse engineers.

Category	Raw Data	Source
Consequences of poor work experience	Poor work experience leads to attrition and burn-out	P11-68
What poor work experience looks like	The constant repetition of the same class of problems and not having the freedom to explore and fix a large class of problems is exhausting. But moving to a higher level of analysis is less exhausting but the rate of recognition for the work you do decreases so there is a tradeoff. You solve fewer problems and get rewards in the same span of time.	P11-36
Attract work that has a high impact	When there was some huge organizational impact for the work he did, there have been some accolades from management chain for that. But that's for the highest profile stuff and there have only been a few opportunities	P4-134
	its frustrating when you are working hard to be impactful but there is no support from management to do that	P10-68
	No meaningful interactions with people (meaningful means that there are intellectual discussions about malware) so his skill set is diminishing over time	P1-28
	Reverse engineers are attracted to the diversity of challenging problems	P2-77, P2-82, P11-26

61

Intra-Organizational > Job Attributes >

Slide 62

Provide opportunities to game with adversary

PR: One job characteristic that attracts reverse engineers is the ability to understand the intent of the adversary and watch the adversarial capabilities evolve. This should be a required characteristic.

Raw Data	Source
Reverse engineers are motivated by trying to understand the intent of the adversary by looking at the binaries and by watching the adversary evolve. Provide these opportunities in the work for continued motivation.	Beta1-43, P4-20, P1(2nd)-41, P1(2nd)-40, P2-85, P1-43, P4-49, P4-48, P4-47, P10-18, P10-17, P2-84

62

Intra-Organizational > Job Attributes >

Slide 63

Sense of Accomplishment and Recognition

PR: Reverse engineers need to have a sense of positive impact for both the sponsors and the organization. Also, another attractive feature of the job is the puzzle / problem solving aspect of the work. This ability to solve difficult problems offers a sense of accomplishment and satisfaction.

Category	Raw Data	Source
ego/satisfaction that comes with solving puzzles	I get a kick out of knowing how it worked	P11-37
ego/satisfaction that comes with solving puzzles	I ask him why 'knowing how it works' drives him and he said part of it is ego (being pleased with his success) and the other part of it is that he just wants to know or has to know. He used to guess and he'd start asking himself how he really knows his guesses are accurate. It's gratifying to know.	P4-45
ego/satisfaction that comes with solving puzzles	The feeling when you figure out something that is really complex is awesome	P4-46
ego/satisfaction that comes with solving puzzles	provides a sense of accomplishment	P3-112, P4-44
Recognition	Without any recognition for your accomplishments from the organization, you don't feel like you are accomplishing anything	P9-46
	I like seeing my work have a direct impact	P1-44
	I like helping sponsors achieve their mission	P11-26

63

Intra-Organizational > Job Attributes >

Slide 64

Appropriate work tasking

PR: Work should be determined by the sponsor's needs but should also fit with the overall team mission. Also, management should be familiar with my work goals to maximize team efficiency.

Sub-category	Raw Data	Source
Setting the work	Historically, the sponsor and reverse engineer set work goals; often times in the absence of management's awareness. Thus, work duplication was possible. To minimize work duplication and improve team efficiency, management may need to be aware of the work goals and tasking being set.	P9-61. Beta1-128, P9-69, P4-94, P1(2nd)-11, P11-59, P4-100, P10-70, P3-44
Minimize business development functional role	Minimize business development (e.g., finding funding) functional roles because reverse engineers claim this is not within the purview of their expertise	P3-106, P6-74, P3-85, P6-63, P3-19.
Research, not operational work	Ensure that task work fits the expertise of the team (e.g., research rather than operational work)	P6-69, P6-77, P4-114, Beta1-126, P8-73, P4-118, P11-34, P6-69, P4-73, P3-18, P4-113

64

Intra-Organizational > Job Attributes >

Slide 65

Performance Metrics

PR: Create new performance metrics that accurately reflect speed and accuracy of work products. Do not use productivity metrics because they often are absent of indicators of quality. While deriving metrics that distinguish novices from experts is challenging, scenario-based metrics are suggested by reverse engineers.

Sub-category	Raw Data	Source
Do not use these metrics	Metrics that don't accurately convey individual performance (e.g., emphasis on work accuracy, well-written reports, opinions are supported, etc.).	P3-39
Do not use these metrics	Attribution metrics	P9-37
Do not use these metrics	No productivity measures independent of quality (e.g., number of reports, number of malicious code files analyzed, number of indicators, etc.) This enforces busy work and not quality work	Beta1-50, P4-121, P4-43, P7-12,
Problems with productivity metrics that are independent of accuracy	This enforces busy work and not quality work	Beta1-50
Problems with productivity metrics that are independent of accuracy	There is a fear that productivity metrics will migrate into producing a certain number of tools per unit of time for customers which is not their expertise	P4-121
Problems with productivity metrics that are independent of accuracy	Not all malware is created with equal complexity. Some malware have unexpected twists that take longer to uncover. Not everyone analyzes the same sample so an assessment of how fast it takes people is not a measure of performance.	Beta1-46
Problems with productivity metrics that are independent of accuracy	Different people can report on the same type of malware sample or different people can report on different aspects of the same sample.	Beta1-52
Problems with productivity metrics that are independent of accuracy	Are you encouraging people to not take a deep dive into the problem space by encouraging speed?	
Problems with productivity metrics that are independent of accuracy	Number of adversarial attacks you blocked is not good because it tells you nothing. If the number goes up,, are you getting attacked more or are you blocking more or both? It makes the organization look foolish	P9-38
Accuracy is most important type of metric		Beta1-33, P10-24, Beta1-46, Beta1-48, P2-32, P4-43, Beta1-50,
Coming up with good metrics is hard; I don't know what the metrics should be.		P9-62, P10-23, P11-19
Try these assessments	Scenario-based assessments	P2-33
Try these assessments	Find the inaccuracies in a report	P2-35, P2-67

Intra-Organizational > Job Attributes >

65

Slide 68

Team structure

PR: The team structure may need to be self-organizing; forming and dissolving based on the work type and on trusting interpersonal relationships.

Sub-category	Raw Data	Source
Should be based on work type		P8-44, P6-55, P7-59, P1-47, P4-69, P3-49, P10-45, Beta1-78
Minimal formal structure	For team leadership, I don't want a lot of structure but I do want to have a general sense of what's going on in the team.	P4-77
Based on interpersonal relationships because these are more effective than assigned teams		Beta1-64, Beta1-65, P9-76, P9-67, Beta1-71
Self organizing teams seems to work best		P4-108, P3-68, Beta1-91, P4-101, P10-40

68

Intra-Organizational > Leadership and Management > within-team leadership and management >

Slide 69

Fosters a culture of feedback and communication

PR: Promote a culture of feedback and constructive communication. Performance feedback, both positive and negative, are important but too much unconstructive negative feedback can lead to lack of collaboration and attrition. Performance feedback is most important from the sponsors but perhaps equally as important from the organization and from peers.

Raw Data	Source
Performance feedback from [stakeholders] is important to me and we need more of it	P9-64, P1-(2nd)-21, P9-72, P11-29, P6-66, P7-33, P9-73
More performance feedback is needed from fellow team members	Beta1-80, P6-20, Beta1-81
Too much critical feedback or competitive feedback can be damaging; stymieing collaboration and leading to a cause of attrition.	P4-50, P4-78, Beta1-97

69

Intra-Organizational > Leadership and Management > within-team leadership and management > team leadership

Slide 70

Is an advocate for the team to senior management

PR: The team leadership (e.g., the team manager) needs to be an advocate for the team with respect to senior management. This leadership needs to convey the expertise and problem space the team works within such that senior management is aware of the value of the team and the value of the work.

Raw Data	Source
Proprietary data omitted	PP6-70,
	P10-71, P6-70
	P11-30, P9-33, P10-65, P9-44, P1(2nd)-28, Beta1-95, P9-34, P9-35, P6-77, P4-114, P8-73, P4-118, P11-34, P7-43, P3-93, P3-55
	P3-90

70

Intra-Organizational > Leadership and Management > within-team leadership and management > team leadership

Slide 71

Enforces performance accountability

PR: The team culture is that of highly accurate, high quality deliverables. When performance is not positively and negatively reinforced, some team members produce sub-par work quality and this leads to friction and demoralization within the team. Ultimately, poor quality work from a single individual reflects negatively on the entire team. Thus, quality work should be positively reinforced and poor quality work, negatively reinforced from the formal leadership.

Proprietary data omitted

Raw Data	Source
	P1-31, P6-49, P4-133, P10-63, P1(2nd)-25

71

Intra-Organizational > Leadership and Management > within-team leadership and management > team leadership

Slide 72

Effective leadership styles

PR: Effective team leadership includes the ability to move between autocratic, democratic, consultative, participative and laissez-faire leadership styles when appropriate. The leadership should have the ability to manage autonomous individuals, build team consensus and also push the team to generate a team vision/mission/strategy that is overtly supported and articulated to senior management within the organization.

Raw Data	Source
For efficient work, an autocratic leadership style is most effective but most demoralizing	P1-49
...the best leadership style is not a single style. The leadership style should move between autocratic, democratic, consultative, participative and laissez-faire when appropriate.	Beta1-96
The leadership must be strong enough to herd cats	P10-60
Must create a team strategy, vision and/or mission and drive that mission	P10-59
The leadership should be engaging with members, transparent with their own work tasks, and not aloof with the team.	P6-68, P4-132, P6-73, P1(2nd)-16,

72

Intra-Organizational > Leadership and Management > within-team leadership and management > team leadership

Slide 73

Facilitate more intra-team collaboration and information sharing

Team collaboration and information sharing is a method to enhance the intellectual capital of the entire team. There are reasons why information sharing is difficult.

Sub-category	Raw Data	Source
Reasons why	It might make problem solving more efficient	P2-38
Reasons why	The team's knowledge grows with sharing	P2-25, P4-75
Hindrances to information sharing	A lack of standardized naming conventions in IDA pro hinders sharing files	Beta1-30, P4-104
Hindrances to information sharing	Conflict: How do we share knowledge of patterns?	P9-19
Hindrances to information sharing	Using standardized terminology in reports to describe malware is needed to facilitate communications	Beta1-56
Reasons why it does not happen	Proprietary data omitted	P2-38

73

Intra-Organizational > Leadership and Management > within-team leadership and management > team leadership

Slide 75

Create directorate mission that values RE

PR: The organization needs to have a mission that includes the mission of the reverse engineering team. Without this, the team lacks fit with the organization and questions its value and importance to the organization. The team strategy should include a budget plan with a funding pipeline plan. The team strategy should also emphasize research (e.g. longitudinal analysis, trends analysis, etc.).

Category	Raw Data	Source
Fit with organizational mission	Ensure the team knows how they fit in with the organization's mission [and] the [directorate's] mission because cynicism about organizational fit occurs	P3-98, P9012
team strategy should include	budget planning	P3-87
team strategy should include	should have a mission that fits with team [directorate] mission and is complimentary to other team missions	P7-37
team strategy should include	should always include research	P2-72
Unify the team under a central vision, mission or strategy	[the strategy] should [include] research on some level	P2-72
	the budget planning should support team objectives	P3-87
	Proprietary data omitted	P9-10
	This should include budgeting, soliciting sponsorship, training, etc.	P6-78

75

Intra-Organizational > Leadership and Management > Senior leadership and management >

Slide 77

Minimize attrition

PR: This job role should minimize the following causal factors which have historically led to burnout and attrition listed below. These factors have been explicitly stated in the interviews to cause burnout and attrition.

Sub-category	Raw Data	Source
Reasons for attrition		P4-137, P4-136, P9-27, P11-69
		P4-139, P4-73,
	Poor work experience, conflicts, not getting personal goals met, personal growth was stymied,	P11-68
		Beta1-98, P4-141
		Beta1-97
		P8-74,
		P11-68, Beta1-97, P11-69
		Beta1-97
		P4-56
		P8-40
		P11-36
		P4-81
	Too busy and too much time pressure	P11-49, P4-83, P9-30, P8-24, P11-33
	Funding lapses,	P11-69
	Metrics do not reflect work quality (e.g., the checkbox driven approach is damaging)	P8-74
		P4-113

Proprietary data omitted

77

Intra-Organizational > Leadership and Management > Senior leadership and management > Support Team

Slide 78

Groom and retain experts

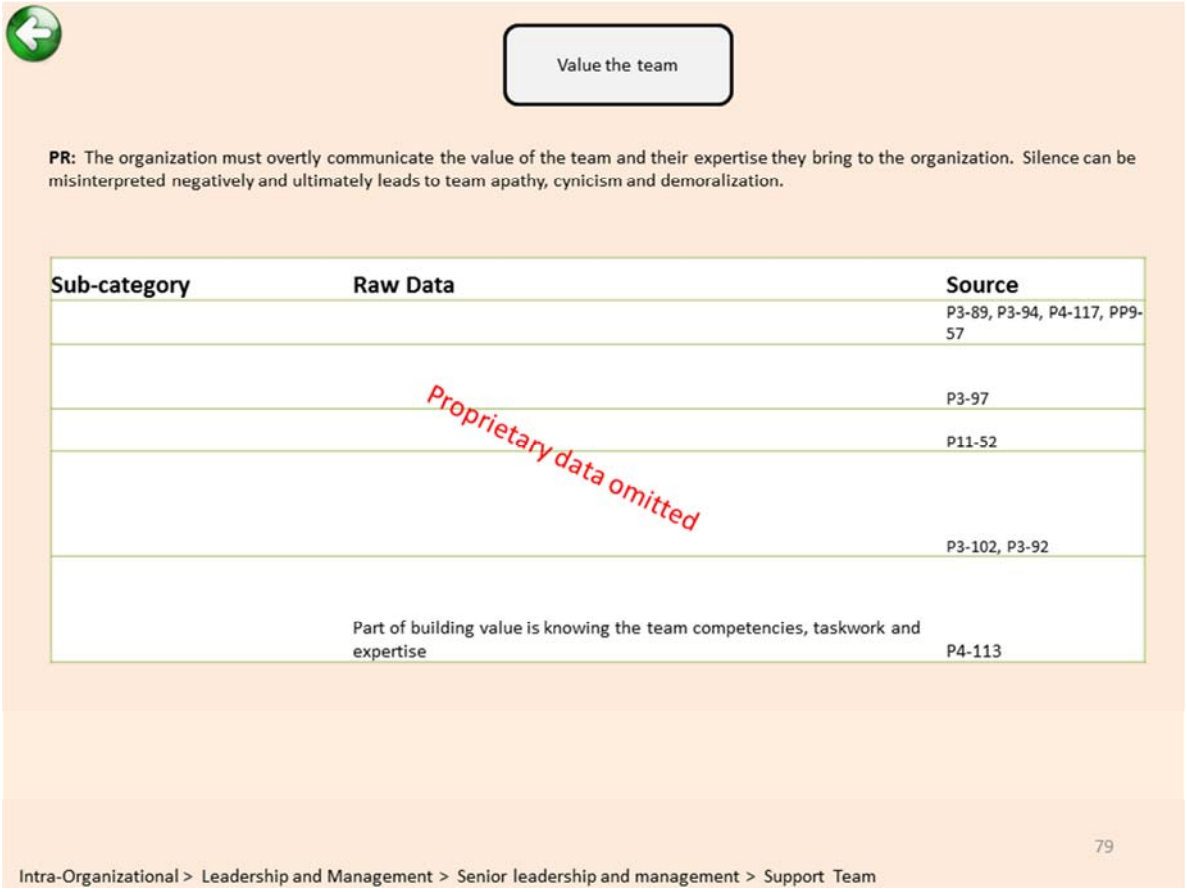
PR: The organization must devise a job role and work context environment that fosters the development and retention of experts.

Category	Raw Data	Source
retain the most senior RE	The most senior people teach junior staff and set the bar for excellence	P9-75
	We need feedback from experts	P1(2nd)-20, P9-74
	Retain experts by attracting the most interesting and technically depth problems for them to work on.	P4-143
	Senior people sometimes know more about what all junior members are working on; providing situation awareness to team leadership	

Intra-Organizational > Leadership and Management > Senior leadership and management > Support Team

78

Slide 79


Value the team
PR: The organization must overtly communicate the value of the team and their expertise they bring to the organization. Silence can be misinterpreted negatively and ultimately leads to team apathy, cynicism and demoralization.
Sub-category
Raw Data
Source
P3-89, P3-94, P4-117, PP9-57
P3-97
P11-52
P3-102, P3-92
Part of building value is knowing the team competencies, taskwork and expertise
P4-113
Proprietary data omitted
79
Intra-Organizational > Leadership and Management > Senior leadership and management > Support Team

Slide 80

Create effective organizational senior management

Effective senior management creates an overall mission statement that reverse engineering fits into. Also effective management tries to understand the nature of the reverse engineering work and team expertise, values and acknowledges the team expertise, removes boulders in the path to development of expertise, and creates a clear communication channel amongst reverse engineers, reverse engineering team leadership and senior management.

Raw Data	Source
	P3-92
	P11-52
	P6-65
	P6-22, P6-18, P3-110, P6-27, P6-25, P7-45, P6-21, P11-80, P6-28, Beta1-23, P10-55, P11-74
	P11-65, P11-78, P11-82, P1(2nd)-35, P7-48, P7-47, P1(2nd)-33, P7-31, P11-81, P2-76, P3-113, P4-128, Beta1-79, P8-71, P3-111
	P1(2nd)-36, P11-50
[Senior management should attract] interesting work for the team, [especially for] the senior most team members. Especially opportunities that allow the team to shine. Lack of stimulating work results in skillset diminishment	P1(2nd)-23, P4-134, P10-68, P1-28
	P3-101, P3-91, P4-72, P11-87
	P11-50
	P11-53, P3-60, P3-104, P11-52, P3-102, P4-117
	P1(2nd)-28, P9-35
	P6-77, P4-114, Beta1-126, P4-118, P4-113
[Senior management should minimizes] an over-engineered work environment that encumbers or stifles work productivity	P9-81, P7-44, P9-79, P7-46, P9-78, P7-43, P1(2nd)-32
	P11-54, P1(2nd)-31, P10-69, P10-67, P11-66, Beta1-127,

Proprietary data omitted

80

Intra-Organizational > Leadership and Management > Senior leadership and management > Support Team

Slide 81

Re-evaluate policies and procedures

PR: The organizational policies and procedures that hinder the development of expertise stated on slide 2 must be re-addressed. Particularly, policies regarding release review, accessing malware in a secure environment, and storing and backing up copies of malware are policies that slow the work flow and deliverable rate to a frustrating degree.

Raw Data	Source
Evaluate policies and procedures that encumber the work flow	P11-65, P11-78, P1(2nd)-36, P11-82, P7-47, P7-48, P7-49, P1(2nd)-34, P1(2nd)-33
Specifically, the release review process encumbers the delivery rate to sponsors.	P7-31, P11-81, P2-76, P3-113, P4-128, P8-71, P3-111, Beta1-79.
Backing up our data is challenging	P7-44
The network breaks all the time [because] it is over-engineered; it requires multiple authentication layers, and malware is not allowed on the network. You cannot run antivirus software on my machine or it will clear out the malware I'm working on.	P7-26, P9-79, P1(2nd)-32, P7-44, P9-81, P9-82,

81

Intra-Organizational > Leadership and Management > Senior leadership and management >

Appendix C Interview Materials

Structured Interview Topics

- Background Information
- Knowledge Requirements
- Critical Incidents
- Contextual Interview
- Personality
- Teamwork
- Organizational Requirements

Background

Job Title	
Number of years working within this job?	
Number of years working as an employee within the computer science discipline?	
Specific expertise you bring to your current job	
Number of years beyond a high school diploma you have been in school	
Highest degree earned	
Describe the work flow you encountered on a daily basis.	
In your opinion, describe factors that differentiate expert from novice performance in this job.	

Knowledge Requirements

Instructions: For the following questions, answer them with respect to what is required for job performance you can be proud to deliver.

- Job knowledge
    - What knowledge (e.g., topics) is required?

- Experience/work history
    - Related Work Experience — Amount of related work experience required to get hired for the job?
    - Any specific experiences required?

- Formal Education
    - What degree is required to perform your job?
    - What course work is relevant?
    - What type of on-the-job training is provided? Apprenticeships? Amount?

- Certifications and licensing requirements?
- Vocational interests
- Hobbies/other interests

Personality

Instructions: For this section, you will only answer based on your own view of what is required for your level of expertise in this job position. When you make ratings, think about all aspects of your job and then make your ratings. You will use two scales to answer each question (e.g., importance, frequency and improvement). If you have a question about the item, please interrupt the facilitator to ask the question. If you wish to elaborate on the point, tell the facilitator to mark the item and then once the survey is complete, discussion is welcome.

Importance	Frequency	Item
		Is calm and self-accepting
		Takes initiative
		Self-motivated
		Displays self-confidence
		Needs or enjoys social interaction
		Is perceptive, tactful and sensitive
		Has a conforming personality
		Shows creativity
		Has an interest in solving problems
		Remains up-to-date with job-related knowledge
		Openness to experience: having wide interests, being imaginative, insightful
		Conscientiousness: Being scrupulous, meticulous, principled behavior and conforming to one’s own conscience
		Extraversion: gregarious, projecting one’s personality outwardly
		Agreeableness: Compliant, trusting, empathetic, sympathetic, friendly, cooperative
		Neuroticism: tendency to become upset or emotional
		Self-esteem: An individual's sense of his or her value or worth, or the extent to which a person values, approves of, appreciates, prizes, or likes him or herself
		Harm avoidance: A tendency towards shyness, being fearful and uncertain, tendency to worry.
		Novelty seeking: Impulsive, exploratory, fickle, excitable, quick-tempered, and extravagant.
		Perfectionism: Socially prescribed perfectionism – "believing that others will value you only if you are perfect." Self-oriented perfectionism – "an internally motivated desire to be perfect.
		The inability to express emotions. "To have no words for one's inner experience"
		Rigidity: Inflexibility, difficulty making transitions, adherence to set patterns
		Impulsivity: Risk taking, lack of planning, and making up one's mind quickly

Importance	Frequency	Item
		Inability or unwillingness to constrain impulses
		Psychoticism: aggressiveness and interpersonal hostility
		Obsessive: Persistent, often unwelcome, and frequently disturbing ideas, thoughts, images or emotions, rumination, often inducing an anxious state.

Teamwork

- Individual vs. Team Structure — Identifies the extent to which employees work in intact teams
    - Percent of Time in Intact Team — Approximately what percentage of your time do you spend working in an intact team? By intact team we mean a group of 3 or more employees who are jointly responsible for whole work processes and work toward shared goals (e.g., production team; development team; project team).

- Are teams homogeneous or heterogeneous with respect to expertise?
- Circle the type(s) of team structure you worked within.

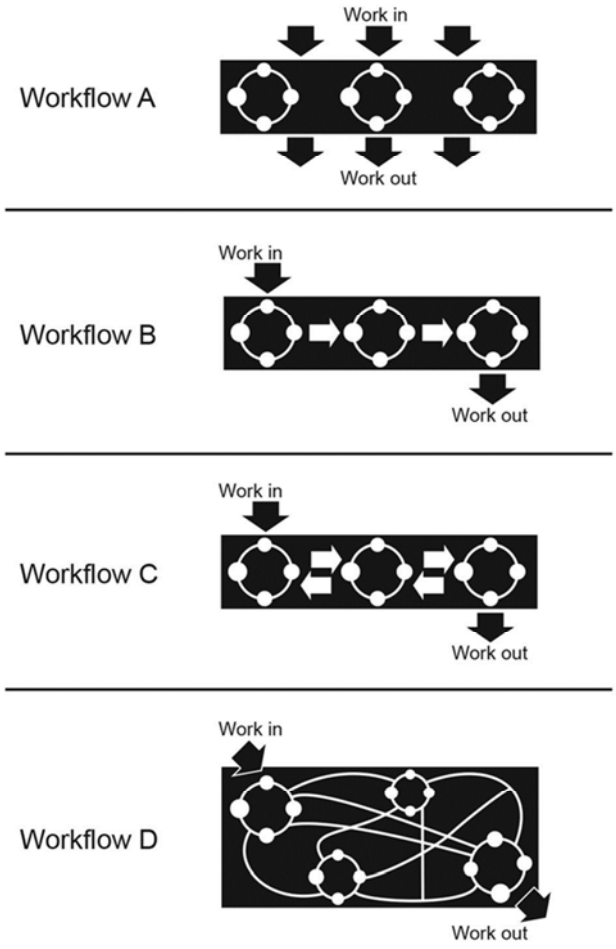


Figure 1: Examples of Teamwork Processes

Please provide frequency and importance ratings for the following with respect to a successful team:

- Team cohesion
- Team Orientation (a person's awareness of self with regard to position, time, place and relationships within the team)
- Team adaptive to dynamic environment
- Team sociability on non-work related topics
- The ability of a team member to voice opinions freely
- The ability of team members to welcome new ideas
- Team leadership sets boundaries for what is acceptable team performance
- Team leadership sets boundaries for what is acceptable team behavior
- The team proactively anticipates negative events that could arise in the future
- The team proactively strategizes tactics that address negative events that are probably to arise in the future
- The team tries to establish group unanaminity and agreements rather than appraising all counter alternatives that may disrupt group agreement
- Team members share team status information to improve performance.
- Team members ensure that other team members understand communications.
- Team back up behavior
- Clear communication is supported and encouraged
- Performance feedback is constructive
- The team coordinates for effective team performance

Describe the leadership of the typical team. Does the team have a clearly identified team lead? What type of leadership does that individual typically display?

Laissez-faire Democratic Participative Consultative Autocratic

Organizational

Instructions: For this section, you will only answer based on your own view of what is required for your level of expertise in this job position. Some of the questions are open-ended and some require you to make ratings on two different scales (e.g., importance and frequency). When you make ratings, think about all aspects of your job first and then make your ratings.

FREQUENCY and IMPORTANCE RATINGS

- Work values
    - Achievement — Occupations that satisfy this work value are results oriented and allow employees to use their strongest abilities, giving them a feeling of accomplishment. Corresponding needs are Ability Utilization and Achievement.
        - Achievement — Workers on this job get a feeling of accomplishment.
    - Working Conditions — Occupations that satisfy this work value offer job security and good working conditions. Corresponding needs are Activity, Compensation, Independence, Security, Variety and Working Conditions.
        - Activity — Workers on this job are busy all the time.
        - Independence — Workers on this job do their work alone.
        - Variety — Workers on this job have something different to do every day.
        - Compensation — Workers on this job are paid well in comparison with other workers in the same team or peer group.
        - Working Conditions — Workers on this job have good working conditions. Please define “good” for the researcher.
        - Workers have job stability
    - Recognition — Occupations that satisfy this work value offer advancement, potential for leadership, and are often considered prestigious. Corresponding needs are Advancement, Authority, Recognition and Social Status.
        - Advancement — Workers on this job have opportunities for advancement.
        - Recognition — Workers on this job receive recognition for the work they do.

- Authority — Workers on this job give directions and instructions to others.

- Social Status — Workers on this job are looked up to by others in their company and their community.

- Relationships — Occupations that satisfy this work value allow employees to provide service to others and work with co-workers in a friendly non-competitive environment. Corresponding needs are Co-workers, Moral Values and Social Service.
  - Co-workers — Workers on this job have co-workers who are easy to get along with.

  - Social Service — Workers on this job have work where they do things for other people.

  - Moral Values — Workers on this job are pressured to do things that go against their sense of right and wrong.

- Support — Occupations that satisfy this work value offer supportive management that stands behind employees. Corresponding needs are Company Policies, Supervision: Human Relations and Supervision: Technical.
  - Company Policies and Practices — Workers on this job are treated fairly by the company.

  - Supervision, Human Relations — Workers on this job have supervisors who back up their workers with management.

  - Supervision, Technical — Workers on this job have supervisors who train their workers well.

- Independence — Occupations that satisfy this work value allow employees to work on their own and make decisions. Corresponding needs are Creativity, Responsibility and Autonomy.
  - Creativity — Workers on this job try out their own ideas.

  - Responsibility — Workers on this job make decisions on their own.

  - Autonomy — Workers on this job plan their work with little supervision.

IMPORTANCE RATINGS ONLY-How important is it to you to have a job that has these qualities

- Organizational Context
    - Decentralization and Employee Empowerment — Indicates the degree to which employees are provided with different types of information and participate in decision-making
        - Have Control Over Unit or Department — You have a great deal of control over what happens in your unit or department
        - Have Influence Over Decisions — You have a great deal of influence over decisions that are made in your unit or department.
        - Monitor Data on Quality/costs/Waste/etc. — You monitor data on quality, costs, waste, and productivity
        - Determine Work Flow or Order of Tasks — You determine work flow or the order in which tasks are performed
        - Invest in New Equipment and Technology — You invest in new equipment and technology
        - Develop New Products, Services, and Procedures — You develop new products, services, and procedures

OPEN-ENDED

- Human Resources Systems and Practices — Organizational practices and policies designed to ensure that an organization has employees who are capable of meeting its goals
    - Recruitment and Selection — Organizational practices, decisions, and processes that affect (a) the capability of an organization to make hiring, promotion, and other personnel decisions, and (b) the number or types of individuals who are willing to apply for or accept a given vacancy
        - Recruitment Operations — Activities involved in implementing recruitment plans (e.g., selecting sources, realistic job preview)
            - Sources of People for Current Job — Which sources are used to recruit people for your current job?
        - Selection Assessment Methods Used — The methods used for selection or promotion of employees

- Assessment Methods Used to Select for Job — Which assessment methods are used to select people for your current job?

- Training and Development — The systematic acquisition of attitudes, concepts, knowledge, roles, or skills that result in improved performance at work

  - Areas of Recent Formal Training — What job-related formal training have you received in the last two years?

- Reward System — Monetary compensation and monetary and non-monetary benefits organizations provide to their employees

  - Compensation Package Components — Which of the following is actually (not theoretically) part of your compensation package (i.e., pay)?
    (a) their knowledge, skills, and performance,
    (b) seniority,
    (c) team performance,
    (d) organizational performance, and
    (e) job attributes

  - Benefits — The extent to which employees' compensation includes benefits such as pensions, insurance, paid leave, awards and bonuses, pay for time not worked, etc.

    - Benefit Components — Which of the following is part of your benefits?
    - pensions,
    - insurance,
    - paid leave,
    - awards and bonuses,
    - pay for time not worked, etc.
    - Other: _____

- Social Processes — A functional subsystem of organization structure subsuming processes linking people (employees) to their work and to each other and includes elements such as values, goals, leadership, and roles
  - Goals — Individual goal setting.
    - Individual Goal Characteristics — The extent to which an individual's goal is made explicit, and the probability that an individual can attain the goal

      - Who sets your work goals? You or your supervisor?

- What kinds of work goals are common to this job? Are they quantitate or qualitative? (e.g., completing X number of activities vs. taking courses at a local university)

- Achieve Most Important Individual Goal — Realistically, the probability that you will achieve your most important individual work goal this year is:

- Goal Feedback — The extent to which an individual is given periodic feedback regarding his or her progress against a goal

    - How Many Specific Individual Goals — What percentage of your individual work goals are specific -- that is, you will know exactly when you have achieved them?

    - When Get Information on Individual Goals — How often do you get information regarding how close you are to achieving your most important individual work goal (for example, an interim financial report or data on number of units sold)?

    - Informal, Job-Relevant Feedback — How frequently do you receive informal, job-relevant feedback from your supervisor?

    - Meet One-on-One With Supervisor on Goals, Training, and Development — During the past year, how often have you met one-on-one with your immediate supervisor to discuss issues such as your performance, goals, training and development?

IMPORTANCE AND FREQUENCY

- Roles — Characteristics of job incumbents' roles, such as the extent to which they involve conflict and overload
    - Role Relationships — Importance of different types of interactions with others both inside and outside the organization
        - Job Interactions — How important are interactions requiring the worker to:
            - Deal With External Customers — How important is it to work with external customers or the public in this job?

            - Coordinate or Lead Others — How important is it to coordinate or lead others in accomplishing work activities in this job?

- Role Conflict — The extent to which an individual has to deal with conflicting demands
    - Often Receive Conflicting Requests — How often do you receive conflicting requests from two or more people at work.
    - Work With Groups With Different Focuses — How often do you work with two or more groups who want you to focus on different things.
    - You and Your Supervisor Agree About Job — How often do you and your supervisor agree about what your job should be.
    - Supervisor Makes Conflicting Requests — How often does your supervisor ask you to do two or more things that conflict (for example, save a large amount of money while at the same time dramatically increasing quality).
- Role Negotiability — The extent to which an individual can negotiate his/her role in an organization
    - Negotiate Changes in Role with Supervisor — How often do you negotiated changes in the nature of your role at work with your supervisor.
    - Significant Input Into Way You Do Job — How often do you have significant input into the way you do your job.
- Role Overload — A discrepancy between the job's demands and one's ability to meet those demands
    - Get Assignments without Adequate Resources — How often do you receive assignments at work without adequate resources and materials to complete them properly.
    - Given Enough Time to Do Work — How often are you given enough time to do what is expected of you at work.
    - Too Much for One Person to Do — How often does it seems like you have too much work for one person to do.

- Task Identity — The extent to which tasks performed on this job can be perceived as contributing to the final product
  - Job Involves Whole Piece of Work — To what extent does your job involve doing a 'whole' and identifiable piece of work? That is, is the job a complete piece of work that has an obvious beginning and end? Or is it only a small part of the overall piece of work, which is finished by other people or automatic machines? (If your job involves many different tasks or pieces of work, try to think about your typical tasks or the tasks you spend the most time on.)
  - Can Do Entire Piece of Work — Your job is arranged so that you can do an entire piece of work from beginning to end.
  - Can Finish What You Start — Your job provides you a chance to completely finish the piece of work you began.
- Autonomy — The amount of freedom in the job, as reflected in a person being able to exercise personal initiative and judgment in task performance
  - Autonomy and Freedom in Job — How much autonomy and freedom are there in your job? That is, to what extent does your job permit you to decide on your own how to go about doing your job?
  - Chance for Initiative and Judgment — Your job gives you a chance to use your personal initiative and judgment in carrying out the work.
  - Opportunity for Independence and Freedom — Your job gives you considerable opportunity for independence and freedom in how you do your job.
- Feedback — The extent to which this job provides information about how well one is performing
  - Extent of Feedback From Doing Job Itself — To what extent does doing the job itself provide you with information about your work performance? That is, does the actual work itself provide clues about how well you are doing--aside from any 'feedback' co-workers or supervisors may provide?
  - Provides Chances for Feedback — Just doing the job provides many chances for you to figure out how well you are doing.
  - After Finishing Job, Know Own Performance — After you finish a job, you know whether you performed well.

OPEN-ENDED

- Job Stability and Rotation — The amount of stability in the job and the extent of job rotation
  - Number of Supervisors in Past Year — How many different supervisors have you had in the past year?
  - Number of Work Teams in Past Year — Approximately how many different work teams have you belonged to during the past year?
  - Number of Work Group Reorganizations in Past Year — In the past year, how many times has your primary work group gone through some kind of reorganization?
  - Number of Times Nature of Job Changed — In the past year, how many times has the nature of your job duties changed dramatically?

IMPORTANCE ONLY

- Culture — Patterns of behaviors and social relationships reflecting the assumptions, values, norms, and artifacts shared by members of the organization
  - Organizational Values — Indicates the importance of different organizational values such as tradition, stability, innovation, and collaboration
    - Guiding Principles of Organization — How important are each of the following concepts, or values, as a guiding principle for your organization as a whole.
      - Taking Chances; Going Out on a Limb — Taking chances; going out on a limb Fairness;
      - Justice — Fairness; justice
      - Precision — Precision; paying attention to even the smallest details
      - Stability — Stability; keeping things on an even keel
      - Getting Things Done — Getting things done; taking decisive or quick action
      - Caring About Employees — Caring about employees; showing concern for their well-being Innovation — Innovation; finding new and better ways of doing things; openness to new ideas

- Aggressiveness — Aggressiveness; forcefully going after what you want

- Valuing Customers — Valuing customers; emphasizing customer service

- Providing High Quality Products — Providing high quality products or services; meeting high standards of excellence

- Openness and Honesty — Openness; honesty; keeping employees well informed

- Flexibility, Adapting to Change — Flexibility, adapting to change Supervisor Role — The nature of supervisory leadership

OPEN-ENDED

- Supervisor Friendly and Supportive — To what extent does your supervisor act in a friendly and supportive manner? For example, does he/she show concern for members of your work group and respect for your ideas?
    - Supervisor Takes Active Role — To what extent does your supervisor take an active role in directing your work group's activities by setting goals, planning and scheduling work, assigning tasks, and making sure that each person knows what he/she should be doing?

    - Supervisor Provides Clear Vision — To what extent does your supervisor provide members of your work group with a clear vision of where the group is going and keep everyone fully committed to the work at hand?

    - Supervisor Solves Problems — To what extent does your supervisor quickly and effectively solve problems, even difficult problems, that come up in your work group?

References

URLs are valid as of the publication date of this document.

[Akgün 2005]
Akgün, A. E.; Byrne, J.; Keskin, H.; Lynn, G. S.; & Imamoglu, S. Z. "Knowledge Networks in New Product Development Projects: A Transactive Memory Perspective." *Information & Management 42*, 8 (December 2005): 1105-1120.

[Anderson 2001]
Anderson, L. W. & Krathwohl, D. R., eds. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. Longman, 2001.

[Arvey 1998]
Arvey, R. D. & Murphy, K. R. "Performance Evaluation in Work Settings." *Annual Review of Psychology 49*, 1 (1998): 141-168.

[Austin 2003]
Austin, J. R. "Transactive Memory in Organizational Groups: The Effects of Content, Consensus, Specialization, and Accuracy on Group Performance." *Journal of Applied Psychology 88*, 5 (October 2003): 866-78.

[Bass 1997]
Bass, B. M. "Does the Transactional-Transformational Leadership Paradigm Transcend Organizational and National Boundaries?" *American Psychologist 52*, 2 (February1997): 130-139.

[Bass 1985]
Bass, B. M. *Leadership and Performance Beyond Expectations.* Free Press, 1985.

[Beyer 1998]
Beyer, H. & Holtzblatt, K. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann, 1998.

[Boyatzis 1982]
Boyatzis, R. E. *The Competent Manager: A Mode for Effective Performance*. John Wiley & Sons, 1982.

[Cannon-Bowers 1995]
Cannon-Bowers, J. A.; Tannenbaum, S. I.; Salas, E.; & Volpe, C. E. Ch. 10, "Defining Team Competencies and Establishing Team Training Requirements," 333-380. *Team Effectiveness and Decision Making in Organizations.* Pfeiffer, 1995.

[Clark 2008]
Clark, R. C. *Building Expertise: Cognitive Methods for Training and Performance Improvement*. Pfeiffer, 2008.

[Cohen 1997]
Cohen, S. G. & Bailey, D. E. "What Makes Teams Work: Group Effectiveness Research from the Shop Floor to the Executive Suite." *Journal of Management 23*, 3 (June 1997): 239-290.

[Costa 1992]
Costa, P.T., Jr. & McCrae, R. R. *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) Manual.* Psychological Assessment Resources, 1992.

[DHS 2012]
Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies. *National Cybersecurity Workforce Framework.*
http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework (2012).

[Dickinson 1997]
Dickinson, T. L. & McIntyre, R. M. Ch. 2, "A Conceptual Framework for Teamwork Measurement," 19-44. *Team Performance Assessment and Measurement.* Lawrence Erlbaum Associates, 1997.

[DoD 2011]
Department of Defense. *S&T Emphasis Areas.*
http://www.acq.osd.mil/chieftechnologist/areas/index.html (2011).

[DoD 2010]
Department of Defense. *Cyber PSC S&T Roadmap.*
http://www.acq.osd.mil/chieftechnologist/publications/docs/
Cyber-PSC_Briefing_DistroA_RE.pdf (November 26, 2010).

[Doverspike 2012]
Doverspike, D. & Arthur Jr., W. Ch. 21, "The Role of Job Analysis in Test Selection and Development," 381 - 400. *The Handbook of Work Analysis: Methods, Systems, Applications and Science of Work Measurement in Organizations*. Routledge, (2012).

[Drouin 2013]
Drouin, N. "How Organizations Support Distributed Project Teams: Key Dimensions and Their Impact on Decision-Making and Teamwork Effectiveness." *Journal of Management Development 32*, 8 (2013): 865 - 885.

[Edwards 2006]
Edwards, B. D.; Day, E. A.; Arthur, W.; & Bell, S. T. "Relationships Among Team Ability Composition, Team Mental Models, and Team Performance." *Journal of Applied Psychology 91*, 3 (May 2006): 727-736.

[Ericsson 2006]
Ericsson, K. A. ed. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, 2006.

[Evans 2010]
Evans K. & Reeder F. A. *Center for Strategic and International Studies*. "Human Capital Crisis in Cybersecurity." 2010. http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity

[Ginnett 1987]
Ginnett, R. C. *First Encounters of the Close Kind: The Formation Process of Airline Flight Crews* (AFIT/CI/NR-87-138D). U.S. Air Force Academy, 1987.

[Gino 2010]
Gino, F.; Argote, L.; Miron-Spektor, E.; & Todorova, G. "First, Get Your Feet Wet: The Effects of Learning from Direct and Indirect Experience on Team Creativity." *Organizational Behavior and Human Decision Processes 111*, 2 (March 2010): 102-115.

[Guzzo 1996]
Guzzo, R. A. & Dickson, M. W. "Teams in Organizations: Recent Research on Performance and Effectiveness." *Annual Review of Psychology 47*, 1 (February 1996): 307-338.

[Halstead 2008]
Halstead, J. B. "Recruiter Selection Model and Implementation Within the United States Army." *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 39*, 1 (December 2008): 93-100.

[Hausdorf 2010]
Hausdorf, P. A., & Risavy, S. D. "Decision Making Using Personality Assessment: Implications for Adverse Impact and Hiring Rates." *Applied H.R.M. Research 12*, 1 (2010): 100-120.

[Jentsch 2001]
Jentsch, F. & Smith-Jentsch, K. A. (2001). Ch. 5, "Assertiveness and Team Performance: More Than "Just Say No," 73 - 94. *Improving Teamwork in Organizations: Applications of Resource Management Training*. CRC Press, 2001.

[Kawakita 1975]
Kawakita, J. *The KJ Method–A Scientific Approach to Problem Solving*. Kawakita Research Institute, 1975.

[Kitchenham 2009]
Kitchenham, B.; Pearl Brereton, O.; Budgen, D.; Turner, M.; Bailey, J.; & Linkman, S. "Systematic Literature Reviews in Software Engineering–A Systematic Literature Review." *Information and Software Technology 51*, 1 (January 2009): 7-15.

[Kuncel 2010]
Kuncel, N. R. & Hezlett, S. A. "Fact and Fiction in Cognitive Ability Testing for Admissions and Hiring Decisions." *Current Directions in Psychological Science 19*, 6 (December 2010): 339-345.

[Lee 2013]
Lee, C. C. & Chang, J. W. "Does Trust Promote More Teamwork? Modeling Online Game Players' Teamwork Using Team Experience as a Moderator." *Cyberpsychology, Behavior and Social Networking 16*, 11 (July 2013): 1 - 7.

[Lievens 2011]
Lievens, F.; Klehe, U. C.; & Libbrecht, N. "Applicant Versus Employee Scores on Self-Report Emotional Intelligence Measures." *Journal of Personnel Psychology, 10*, 2 (2011): 89-95.

[Lim 2006]
Lim, B. C. & Klein, K. J. "Team Mental Models and Team Performance: A Field Study of the Effects of Team Mental Model Similarity and Accuracy." *Journal of Organizational Behavior 27*, 4 (May 2006): 403-418.

[Marks 2000]
Marks, M. A.; Zaccaro, S. J.; & Mathieu, J. E. "Performance Implications of Leader Briefings and Team-Interaction Training for Team Adaptation to Novel Environments. *Journal of Applied Psychology 85*, 6 (December 2000): 971-986.

[Mathieu 2000]
Mathieu, J. E.; Heffner, T. S.; Goodwin, G. F.; Salas, E.; & Cannon-Bowers, J. A. "The Influence of Shared Mental Models on Team Process and Performance." *Journal of Applied Psychology 85*, 2 (April 2000): 273-283.

[McIntyre 1995]
McIntyre, R. M. & Salas, E. "Measuring and Managing for Team Performance: Emerging Principles from Complex Environments," 9-45. *Team Effectiveness and Decision Making in Organizations*. Pfieffer, 1995.

[McKendrick 2013]
McKendrick, R.; Shaw, T.; de Visser, E.; Saqer, H.; Kidwell, B.; & Parasuraman, R. "Team Performance in Networked Supervisory Control of Unmanned Air Vehicles: Effects of Automation, Working Memory and Communication Content." *Human Factors* (July 13, 2013).

[Nickels 1995]
Nickels, B. J.; Bobko, P.; Blair, M. D.; Sands, W. A.; & Tartak, E. L. *Separation and Control Hiring Assessment (SACHA): Final Job Analysis Report*. *Federal Aviation Administration*, 1995.

[Nyfield 1983]
Nyfield, G. R.; Kandola, R. S.; & Saville, P. F. *The Selection of Air Traffic Controllers: Concurrent Validity Study*. Saville and Holdworth Ltd., 1983.

[Sanders 1987]
Sanders, M. S. & McCormick, E. J. *Human Factors in Engineering and Design*. McGraw-Hill, 1987.

[Seamster 2001]
Seamster, T. L. & Kaempf, G. L. Ch. 2, "Identifying Resource Management Skills for Airline Pilots," 9 - 30. *Improving Teamwork in Organizations: Applications of Resource Management Training*. CRC Press, 2001.

[Shapiro 2013]
Shapiro, J.; Quinn, J.; & Barnes-Farrell, J. L. *Rail Industry Job Analysis: Passenger Conductor* (IPAC TR-2012-01). U.S. Department of Transportation, Federal Railroad Administration, 2013. http://ntl.bts.gov/lib/48000/48100/48182/
TR_Rail_Industry_Job_Analysis_Passenger_Conductor_.pdf

[Sikorski 2012]
Sikorski, M.; Honig, A.; & Lawler, S. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012.

[Stabile 2002]
Stabile, S. J. "Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost?" *U. Pa. Journal of Labor and Employment Law 4*, 2 (2002): 279-313.

[Tannenbaum 2012]
Tannenbaum, S. I.; Mathieu, J. E.; Salas, E.; & Cohen, D. "Teams Are Changing: Are Research and Practice Evolving Fast Enough?" *Industrial and Organizational Psychology 5*, 1 (March 2012): 2-24.

[Thomas 2006
Thomas, S. L. & Scroggins, W. A. "Psychological Testing in Personnel Selection: Contemporary Issues in Cognitive Ability and Personality Testing." *Journal of Business Inquiry: Research, Education, and Application 5* (2006): 28-38.

[Voss 1995]
Voss, J. F.; Wiley, J.; & Carretero, M. Acquiring Intellectual Skills." *Annual Review of Psychology 46*, 1 (February 1995): 155-181.

[White 2005]
White, L. A.; Young, M. C.; Kubisiak, U. Christian; Horgen, Kristen E.; Connell, Patrick W.; Lentz, Elizabeth; Xu, Xian; Borman, Walter C. *Concurrent Validation of the NLSI for U.S. Army Drill Sergeants* (Study Note 2006-01). United States Army Research Institute for the Behavioral and Social Sciences, 2005.

[Yilmaz 2013]
Yılmaz, O. "Effects of Individual Success on Globally Distributed Team Performance." *eprint arXiv:1308.0818* (August 2013).

[Zhang 2007]
Zhang, Z.-X.; Hempel, P. S.; Han, Y.-L.; & Tjosvold, D. "Transactive Memory System Links Work Team Characteristics and Performance." *Journal of Applied Psychology 92*, 6 (November 2007): 1722-1730.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Job Analysis Results for Malicious-Code Reverse Engineers: A Case Study	FA8721-05-C-0003

6. AUTHOR(S)

Jennifer Cowley

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2014-TR-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Recently, government and news media publications have noted that a large-scale military cyberattack against the United States will be crippling primarily because of the existing personnel shortages and expertise gaps in the cybersecurity workforce. One critical job role within cyber defense teams is the malicious-code reverse engineer who deconstructs malicious code to understand, at the binary level, how the malware behaves on a network. Given the severe staffing shortages of these engineers, efforts to identify individual traits and characteristics that predict the development of expertise is important. Currently, job analysis research on teams of malicious-code reverse engineers is lacking. Therefore, a job analysis was conducted to identify individual factors (e.g., cognitive abilities, knowledge, and skills) and team factors (e.g., team leadership, decision making) that enable, encumber, or halt the development of malicious-code reverse engineering expertise. A 10-member malicious-code reverse engineering team was interviewed using a contextual inquiry/semi-structured interview hybrid technique to collect job analysis information. Performance factors were inferred based on the raw interview data.

The results indicate that expert performance requires other non-domain-specific knowledge and skills (e.g., performance monitoring, oral and written communication skills, teamwork skills) that enable successful performance. Expert performance may be enabled by personality factors (i.e., conscientiousness) and cognitive abilities (i.e., working memory capacity). Attributes of successful novices were also collected. Subsequent research will empirically validate that these factors predict the development of expertise. Training and operations implications for this research are also detailed.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Job Analysis, Malicious code Reverse Engineers, Expert	114

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL